VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Axiomatické teorie množin

Axiomatic Set Theories.

2014 Bc. Martin Nemček

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Zadání diplomové práce

Student: **Bc. Martin Nemček**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2612T025 Informatika a výpočetní technika

Téma: Axiomatické teorie množin
Axiomatic Set Theories.

Zásady pro vypracování:

Student zpracuje dostupnou literaturu k tomuto tématu tak, aby výsledný text mohl být použit pro výuku v předmětu "Vybrané partie z logiky". Přínos studenta bude tedy spočívat v tom, že vypracuje přehlednou studii doplněnou o příklady a důkazy jednotlivých teorémů.

Práce bude obsahovat:
1. Definici logické teorie (jazyk, axiomy, důkazový kalkul).
2. Přehled jednotlivých teorií množin.
3. U každé teorie uvede student názorné příklady a důkazy teorémů tak, aby text mohl být použit pro výuku v předmětu "Vybrané partie z logiky".

Seznam doporučené odborné literatury:

[1] Sochor Antonín: Matematematika teorií množin. Praha: Karolinum 2006
[2] Cohen Paul J.: Set Theory and the Continuum Hypothesis. New York: Dover Publications, Inc., 2008
Dále dle pokynů vedoucího diplomové práce.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **doc. RNDr. Marie Duží, CSc.**

Datum zadání: 01.09.2013
Datum odevzdání: 07.05.2014

doc. Dr. Ing. Eduard Sojka
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 5. května 2014 ....

Poďakovanie

Touto cestou by som chcel poďakovať vedúcej práce doc. RNDr. Marii Duží, CSc. za cenné rady, odborné vedenie a inšpiráciu pri tvorbe tejto diplomovej práce.

Abstrakt

Práce je zaměřena na axiomatické teorie množin. Jsou v ní přehledně zpracovány a popsány nejznámější teorie jako Zermelo-Fraenkelova teorie množin, Gödel-Bernaysova teorie množin a Kelley-Morseova teorie množin. V úvodu je popsána výstavba logické teorie s definicí základních pojmů a principů. Dále je zde zhrnut a objasněn důvod vzniku axiomatických teorií množin a důvod, proč naivní teorie množin nebyla dostačující. Další kapitoly jsou zaměřeny na důkazy jednotlivých teorémů u konkrétních teorií množin. Jedna z těchto kapitol je zaměřena na zdůvodnění, proč můžeme tvrdit, že Kelley-Morseova teorie množin je silnější než Zermelo-Fraenkelova teorie množin. Další kapitola popisuje, jakým způsobem omezit Gödel-Bernaysovu teorii množin na teorii s konečným počtem axiomů, i když se tato teorie standardně považuje za nekonečně axiomatizovatelnou. Poslední kapitola je věnována důležitým důkazům bezespornosti axiomu výběru a hypotézy kontinua se Zermelo-Fraenkelovou teorií množin.

Klíčová slova: axiom, množina, třída, formule, teorie, důkaz, teorie množin

Abstract

Thesis focuses on axiomatic set theories. There are clearly described and processed the most famous theories - Zermelo-Fraenkel set theory, Gödel-Bernays set theory and Kelley-Morse set theory. In introduction is described the construction of logical theory with the definition of basic concepts and principles. There is also summarized and explained the cause of formation the axiomatic set theory and why naive set theory was not sufficient. Next chapters focus on proofs of individual theorems in specific theories. One of these chapters focuses on the rationale, why we can say that the Kelley-Morse set theory is stronger than Zermelo-Fraenkel set theory. Another chapter describes, how is possible to limit Gödel-Bernays set theory to theory with a finite number of axioms, although this theory is normally considered as infinitely axiomatized. The last chapter is dedicated to important proofs of unequivocalness of axiom of choice and the continuum hypothesis with Zermelo-Fraenkel set theory.

Keywords: axiom, set, class, formula, theory, proof, set theory

Seznam použitých zkratek a symbolů

FGB	–	Finitná verzia Gödel-Bernaysovej teórie množín
GB	–	Gödel-Bernaysova teória množín
KM	–	Kelley-Morseova teória množín
ZF	–	Zermelo-Fraenkelova teória množín

Obsah

1 Úvod

Teória množín, ktorej počiatky siahajú do 19. storočia, výrazným spôsobom zasiahla vývoj matematiky v 20. storočí. Za zakladateľov teórie množín môžeme považovať Bernarda Bolzana (1781-1848), ktorého prínos nebol dlhú dobu úplne docenený a hlavne Georga Cantora (1845-1918), ktorý publikoval svoju prvú prácu z oblasti teórie množín v roku 1872 a postupom času vytvoril teóriu, na ktorej základoch stojí súčasná teória množín. Jeho intuitívne poňatie množiny však spôsobovalo, že teória množín musela už od svojho vzniku zápasit' s istými ťažkosťami, keďže množinu formuloval ako súhrn predmetov, objektov, ktoré sú dobre rozlíšiteľné našou mysľou alebo intuíciou. Táto formulácia bola tak všeobecná a neurčitá, že prípustnosť tvorenia množín z objektov nijako neusmerňovala a umožňovala neobmedzenú možnosť takejto tvorby. Takto mohla vzniknúť aj taká množina, akou bola napríklad množina všetkých množín, ktorej existencia bola však sporná. Východiskom, ktoré sa v tejto situácií ponúkalo, bolo vybudovanie teórie množín pomocou axiomatickej metódy.

Každú matematickú teóriu je možné pokladať za sústavu výrokov o nejakých matematických objektoch. Pri získavaní poznatkov sa v matematike postupuje deduktívne, ale je zrejmé, že každý poznatok nie je možné odvodiť z nejakého iného (napríklad jednoduchšieho) poznatku. Preto je vhodné vychádzať z istých tvrdení (axiómov), ktoré prehlásime za pravdivé. Axiómy teda formulujú isté vlastnosti základných pojmov, ktoré ďalej nedefinujeme a pokladáme ich za hotové a z nich potom odvodzujeme prostredníctvom prípustných logických prostriedkov ďalšie poznatky. Týmto spôsobom je možné vybudovať celú teóriu. Moderná axiomatická metóda sa od pôvodnej klasickej (ktorej základy položil Euklides pri budovaní axiomatického systému geometrie) odlišuje tým, že svoj jazyk aj logický aparát buduje súčasne. Axiómy tu teda nie sú chápané ako nejaké samozrejmosti (napríklad bod alebo priamka v geometrii), ale sú považované za východiská, na ktorých je celá teória vybudovaná.

V ďalšom texte sa budeme zaoberať tromi konkrétnymi axiomatickými teóriami množín, ktoré budeme skúmať. Prvou, základnou a najrozšírenejšou je Zermelo - Fraenkelova teória množín, ktorá vychádza z práce Ernsta Zermela (1871 - 1953), na ktorú nadviazal Adolf Fraenkel (1891 - 1965) a dal teórií konečný tvar. Neskôr vzniká ďalšia axiomatika - Gödel-Bernaysova teória množín, ktorú Paul Bernays (1888 - 1977) založil na pojme *trieda*, čím popri pojme množina rozšíril základnú terminológiu a tak umožnil manipulovať s dvomi rozdielnymi entitami - triedami a množinami. Kurt Gödel (1906 - 1978) túto teóriu doplnil tým, že ztotožnil triedy s množinami, ktoré majú rovnaké prvky a tým dal tejto teórií definitívnu formu, v ktorej sa nachádza dnes. Poslednou axiomatickou teóriou, ktorou sa budeme zaoberať, je Kelley-Morseova teória množín, ktorej základy položil Anthony Morse (1911 – 1984) na svojej prednáške v roku 1939 na ktorú nadviazal John Kelley (1916 - 1999) a doplnením vo svojej práci dal tejto teórií výslednú podobu. Táto teória je podobná teórií GB, rozdiel spočíva v jedinom axióme, pričom táto zmena má na celú teóriu podstatný vplyv. Uvedené teórie množín preskúmame, uvedieme v nich dôkazy niektorých teorémov, ktorých dôsledky zkonštatujeme na záver.

V konečnom dôsledku, v súčasnosti môžeme bezpochyby tvrdiť, že teória množín zasiahla neskorší vývoj matematiky vo viacerých smeroch. Spustila aktívny záujem o štúdium otázok týkajúcich sa rozvoja poznávania v matematike, čím vytvorila nevyhnutné predpoklady pre vznik nových dôležitých matematických disciplín, ktorými sú napríklad teória reálnych funkcií, topológia a funkcionálna analýza, bez ktorých si nie je možné predstaviť modernú matematiku.

2 Definícia logickej teórie

Na úvod musíme uviesť, že pojmy, axiómy a odvodzovacie pravidlá môžu byť definované viacerými ekvivalentnými spôsobmi, preto sa ich definíciou budeme zaoberať v nasledujúcom texte. Neskôr, v ďalších kapitolách, si budú konkrétne dôkazy jednotlivých teorémov zase vyžadovať overenie niektorých tvrdení pre každé odvodzovacie pravidlo a každý axióm samostatne. Axiómy a odvodzovacie pravidlá logiky je vhodné popisovať s možnosťou viacerých druhov premenných hneď od začiatku, keďže napríklad v axiomatických teóriách množín pracujúcich s triedami sa pre prvky vyskytujú dva druhy premenných - množinové premenné a triedne premenné.

K základným pojmom, s ktorými budeme manipulovať, patrí: **predikát**, ktorý je definovaný pri ňom uvedenou početnosťou. Špecifickými predikátmi sú napríklad $\in$, ktorý interpretuje vzťah náležania alebo $=$ pre rovnosť. Ďalším pojmom, s ktorým budeme manipulovať, sú **premenné** rôznych druhov, pričom sú rozdelené do rozdielnych skupín a platí, že premenné v jednej skupine zastupujú jeden druh premenných. Treba pripomenúť, že jedna premenná môže zastupovať viac druhov. Použitými symbolmi premenných budú napríklad x, y, X, Y, pričom použitie veľkých a malých písmen si vyžaduje rozlíšenie množín a tried v niektorých teóriách množín, s ktorými budeme pracovať. Ďalej potrebujeme symboly pre **funkcie**, ktoré taktiež definuje početnosť pri nich uvedená. Špeciálnymi symbolmi $Dom, \Im$ sú označované viacpočetné funkcie. Pre niektoré poradie druhov objekov je výsledkom funkcie objekt určitého druhu (k n-árnej funkcii môžu byť určené (n+1)-tice druhov premenných). Funkcia s početnosťou 0 je definovaná ako **konštanta**. Konštanta môže byť určená, akého je druhu. Špecifické konštanty a funkcie sú značené $\cap, \cup, \bigcup, \aleph_\alpha$. Použitými **kvantifikátormi** budú všeobecný ($\forall$) a existenčný ($\exists$). Ďalšími používanými základným entitami sú **spojky** negácie ($\neg$), konjunkcie ($\wedge$), disjunkcie ($\vee$), implikácie ($\rightarrow$) a ekvivalencie ($\equiv$).

2.1 Termy

Označujú sa $t, T, ...$. Môžu mať definované, do ktorého druhu ktorý term patrí a jeden term môže byť súčasne viacerých druhov. Každý znak pre premennú a konštantu je tiež termom a aj $Dom(t_1, ..., t_n)$ je term, ak Dom označuje funkciu s početnosťou n a $t_1, ..., t_n$ sú tiež termy.

2.2 Formule

Formule sa značia $\alpha, \varphi, \psi, \Phi, \Psi, ...$ a dostaneme ich iterovanou aplikáciou pravidiel:

- $P(t_1, ..., t_n)$ je formulou, ak P je predikát početnosti k a $t_1, ..., t_n$ sú termy
- ak sú α, β formule, sú aj $\neg\alpha$, $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \rightarrow \beta)$ a $(\alpha \equiv \beta)$ formulami
- ak je α formula a x je premenná ľubovoľného druhu, sú aj $(\forall x)\alpha$ a $(\exists x)\alpha$ formulami

Term t je substituovateľný za premennú x vo formuli α, ak je premenná x voľná (nie je viazaná žiadnym kvantifikátorom) vo formuli α, pričom substituujeme všetky jej voľné výskyty, ďalej ak sa žiadna individuová premenná termu t nestane po vykonaní substitúcie viazanou vo formuli α a ak je term t druhu premennej x.

Potom značíme $\alpha(x/t)$.

2.3 Jazyk

Je tvorený abecedou (symbolmi) a gramatikou a vytvárame ho aplikovaním pravidiel gramatiky na symboly abecedy. Súčasťou jazyka je aj zadanie početností jednotlivých predikátov, funkcií a konštánt a prípadne rozdelenie premenných do skupín druhov premenných.

Jazyk teórie množín potrebujeme dopĺňať o nové symboly funkcií, konštanty, predikáty a nové druhy premenných. Obohacovanie jazyka sa riadi nasledujúcimi predpismi:

- **Zadefinovanie funkcie:** Nech T je teória s rovnosťou. Nech je napríklad $\alpha(y, x_1, ..., x_n)$ formula (ktorá nemá iné voľné premenné ako (niektoré z) $y, x_1, ..., x_n$) taká, že $T \vdash (\exists!$ (=existuje práve jeden) $y)\alpha(y, n_1, ..., n_n)$ pre akékoľvek premenné $n_1, ..., n_n$ ľubovoľného druhu, ktoré sa nevyskytujú vo formuli α (v prípade, že by existoval len univerzálny druh premenných v jazyku teórie T, tak by stačilo požadovať len $T \vdash (\exists!y)\alpha(y, x_1, ..., x_n)$, pričom by $x_1, ..., x_n$ boli tohto univerzálneho druhu). Ak je T' rozšírením teórie T pridaním novej n-árnej funkcie $\Im$ k jazyku teórie T (ktorej hodnota je vždy práve druhu premennej y) a axiómami $y = \Im(n_1, ..., n_n) \equiv \alpha(y, n_1, ..., n_n)$, potom je teória T' konzervatívnym rozšírením (každá formula jazyka teórie T dokázateľná v T' je dokázateľná aj v T) teórie T. Ku každej formuli β jazyka teórie T' existuje formula β' jazyka teórie T tak, že platí $T' \vdash \beta \equiv \beta'$.

- **Zavedenie konštanty:** Nech pre nejakú formulu $\alpha(x_1, ..., x_k)$ platí $T \vdash (\exists x_1, ..., x_k)\alpha$. Ak je rozšírením teórie T teória T' vzniknutá pridaním od seba rozličných nových konštánt $c_1, ..., c_k$ k jazyku teórie T, kde sú tieto konštanty po rade práve druhov reprezentovaných premennými $x_1, ..., x_k$ a pridaním axiómu $\alpha(x_1/c_1, ..., x_k/c_k)$, potom je teória T' konzervatívnym rozšírením teórie T.

- **Zadefinovanie druhu premenných:** Nech platí: Formula α má jednu voľnú premennú x, teória T je teóriou s rovnosťou a $T \vdash (\exists x)\alpha$. Ak je teória T' rozšírením teórie T vzniknutým pridaním nového druhu premenných $u, ...$ k jazyku teórie T a pridaním axiómu $(\forall x)[(\exists u)(u = x) \equiv \alpha]$, pričom každý term druhu u je tiež druhu x, potom je teória T' konzervatívnym rozšírením teórie T a ku každej formuli β jazyka teórie T', v ktorom sú voľné výskyty premenných druhu u, existuje formula β' v jazyku teórie T, pre ktorú platí $T' \vdash \beta \equiv \beta'$.

- **Zadefinovanie predikátu:** Nech je $\alpha(x_1, ..., x_k)$ formulou jazyka teórie T, ktorá nemá iné premenné, ako $x_1, ..., x_k$, pričom nemusí mať všetky. Rozšírením teórie T pridaním nového k-árneho predikátu P a axiómov $P(n_1, ..., n_k) \equiv \alpha(n_1, ..., n_k)$ (kde

$n_1, ..., n_k$ sú premenné ľubovoľných druhov, ktoré sa nevyskytujú vo formuli α) k jazyku teórie T získame rozšírenie T' teórie T. Potom je teória T' konzervatívnym rozšírením teórie T a pre každú formulu β jazyka teórie T' existuje taká formula β' jazyka teórie T, že platí $T' \vdash \beta \equiv \beta'$.

2.4 Teória

Teória je definovaná jazykom, ktorý používa a systémom formúl vytvorených v tomto jazyku, ktoré sú pomenované ako *axiómy teórie*.

2.5 Axiómy logického kalkulu

Sú to všetky formule, ktoré sú v niektorom z nasledujúcich tvarov, pričom formule skúmaného jazyka sú označené symbolmi α, β, γ, symboly $x, x_1, ..., x_n, y_1, ..., y_n$ reprezentujú premenné akéhokoľvek druhu, P je v úlohe predikátového symbolu a $\Im$ značí funkciu.

- $\alpha \to (\beta \to \alpha)$

- $[\alpha \to (\beta \to \gamma)] \to [(\alpha \to \beta) \to (\alpha \to \gamma)]$

- $(\neg\alpha \to \neg\beta) \to (\beta \to \alpha)$

- $(\forall x)\alpha \to \alpha(x/t)$ - *Axióm špecifikácie* (*substitúcie*) - za predpokladu, že term t je substituovateľný za premennú x vo formuli α

- $(\forall x)(\alpha \to \beta) \to (\alpha \to (\forall x)\beta)$ - *Axióm distribúcie* - za predpokladu, že premenná x nemá vo formuli α voľný výskyt

- $x = x$ - *Axióm identity*

- $(x_1 = y_1 \wedge ... \wedge x_n = y_n \wedge P(x_1, ..., x_n)) \to P(y_1, ..., y_n)$
  - V jazyku teórie množín je možné tento axióm pre predikáty $=$ a $\in$ postupne formulovať' nasledovne:
  - $x = n \to n = x$ (symetria rovnosti)
  - $(x = n \wedge n = y) \to x = y$ (tranzitivita rovnosti)
  - $(x = n \wedge n \in y) \to x \in y$
  - $(x = n \wedge y \in n) \to y \in x$

- $(x_1 = y_1 \wedge ... \wedge x_n = y_n) \rightarrow \Im(x_1, ..., x_n) = \Im(y_1, ..., y_n)$

Posledné tri axiómy sa označujú ako *Axiómy rovnosti*, ak symbol $=$ označuje predikát rovnosti, ktorý je možné použit' iba v teóriách s rovnosťou. K **dedukčným pravidlám** radíme odlučovacie pravidlo *modus ponens*, ktoré umožňuje vyvodit' formulu β z formulí α a $\alpha \rightarrow \beta$ a pravidlo *generalizácie* dovoľujúce pre premennú x, ktorá môže byt' akéhokoľvek druhu, odvodit' formulu $(\forall x)\alpha$ z formule α.

2.6 Dôkazy

Dôkaz je konečná postupnost' krokov, tj. podľa gramatiky jazyka dobre vytvorených formúl, z ktorých je každá buď axióm alebo vznikne pomocou odvodzovacieho pravidla z predchádzajúcich dobre vytvorených formúl, pričom posledným krokom tejto postupnosti je dokazovaná formula. Aby bola formula dokázateľná v určitej teórií, musí byt' jej členom a musí v nej existovat' jej dôkaz. Označenie $T \vdash \alpha$ sa použije, ak je formula α dokázateľná v teórií T. Ak pre nejakú formulu α v určitej teórií existuje dôkaz formule $(\alpha \wedge \neg\alpha)$, je táto teória sporná. Teória sa nazýva *bezosporná*, ak sa takýto dôkaz v nej nenachádza.

Pri spracovaní tejto kapitoly sme čerpali zo zdrojov [3], [2].

3 Úvod do axiomatických teórií množín

Za základné a ďalej nedefinované entity modernej matematiky môžeme považovať množiny a neobvyklé je práve to, že až v druhej polovici 19. storočia sa začali systematicky skúmať. Ale ani v súčasnosti nie je štandardný postup pri štúdiu určitej oblasti začínať množinami.

Zakladateľom teórie množín je Georg Cantor (1845-1918), ktorý svoj výskum založil na prácach nemecky hovoriaceho čecha Bernarda Bolzana (1781-1848). Ucelením poznatkov o množinách a vznikom ich teórie sa otvorila cesta pre vznik a neskôr rozvoj moderných matematických disciplín, ktorými sú napríklad všeobecná algebra alebo funkcionálna analýza. Cantorova naivná teória množín bola založená na intuícii a dostal sa s výskumom pomerne ďaleko. Avšak ako výskum pokračoval, začali sa objavovať určité nezrovnalosti, v terminológií matematickej logiky spory, ktoré boli pomenované ako *paradoxy* [1]. Prvým bol v roku 1897 Burali-Fortiov paradox, nasledujúci objavil v roku 1899 sám Cantor a znie takto: „Uvažujme množinu U všetkých množín, potom množina $P(U)$ všetkých jej podmnožín obsahuje viac prvkov, ako množina U“. Toto paradoxné tvrdenie vychádza z tzv. **Cantorovej vety**:

Věta 3.1 *Potenčná množina $P(X)$ (obsahujúca všetky podmnožiny) množiny X obsahuje viac prvkov, ako množina X.*

Důkaz. Toto tvrdenie je ekvivalentné tvrdeniu, že neexistuje surjektívne zobrazenie množiny X na množinu $P(X)$. Nech existuje surjektívne zobrazenie $f : X \to P(X)$. Pre každý prvok (tj. množinu) $A \in P(X)$ existuje nejaký prvok $x \in X$ tak, že $f(x) = A$. Nech existuje podmnožina $Y \subset X$ taká, že $Y = \{x \in X : x \notin f(x)\}$. Množina Y obsahuje tie prvky množiny X, ktoré nie sú vo svojom obraze definovanom zobrazením f. Množina Y je zrejme podmnožinou množiny X, takže musí existovať prvok $y \in X$ taký, že $Y = f(y)$. Z toho vyplývajú dve situácie:

- ak $y \in Y$, potom ale prichádzame ku sporu s definíciou Y, podľa ktorej $y \notin f(y)$, ale $f(y) = Y$

- ak $y \notin Y$, potom ale opäť prichádzame ku sporu s definíciou Y, podľa ktorej $y \in Y$

Takže množina $P(X)$ obsahuje vždy viac prvkov ako množina X, keďže existencia surjektívneho zobrazenia $f : X \to P(X)$ vedie ku sporu. ∎

Príliš uvoľnené pojatie pojmu množina, ktorú Cantor popísal ako akýkoľvek súhrn vzájomne odlíšiteľných objektov, bolo príčinou tohto i ďalších paradoxov. Pritom ale platí, že ľubovoľný objekt univerza sa dá jednoznačne definovať, či do skúmanej množiny patrí alebo nie. Ďalším faktom, ktorý Cantor prijal za axióm bolo, že množinu tvorí akýkoľvek súhrn prvkov s identickou vlastnosťou. „Byť množinou“ je samozrejme tiež vlastnosť, takže je podľa jeho teórie možná aj množina M všetkých množín, ktorá, ako sme si dokázali, je sporná. Spočiatku sa paradox objavený Cantorom nepovažoval za až tak závažný, pretože bol až na okraji obvyklých matematických úvah, ale keď sa na scéne objavil Bertrand Russel (1872-1970) so svojím paradoxom, situácia sa skomplikovala, pretože jeho

[1] Podobné nezrovnalosti boli známe už v staroveku ako rôzne antinómie (výpoveď, z ktorej ak predpokladáme jej pravdivosť, odvodíme jej nepravdivosť a naopak).

paradox manipuluje s jednou zo základných operácií na množinách - náležaním ($\in$). Jeho znenie je nasledujúce: Uvažujme množinu M všetkých takých množín, ktoré nie sú svojím vlastným prvkom. Potom odpoveď na otázku, či je množina M prvkom seba samej, vedie ku sporu. Zo zápisu $M = \{X \mid X \notin X\}$ vyplýva, že $M \in M \Leftrightarrow M \notin M$. Význam pýtať sa, či $M \in M$ vyplýva z korektného zadefinovania množiny M. Paradox objavený Russelom bol pre ľahšie pochopenie interpretovaný ako *Paradox holiča*. Znie takto: V určitej obci prikáže starosta miestnemu holičovi, aby holil práve všetkých tých mužov, ktorí sa neholia sami. Otázkou je, či sa má holič oholiť sám alebo nie. Vo formálnom zápise:

Nech $a \in b$ znamená, že muž *a* holí muža *b*. Takže podľa nariadenia starostu $h \in x \Leftrightarrow x \notin x$, z čoho pre $x = h$ dostaneme spor.

Existujú aj iné typy paradoxov, tzv. *sémantické*. Jedným takým je aj súvetie „Nasledujúca veta je nepravdivá. Predchádzajúca veta je pravdivá." Taktiež aj výrok: „Táto veta je nepravdivá."

Použitie pravidla autoreferencie [2] je príčinou takýchto paradoxov. Môžeme povedať, že tu dochádza k prelínaniu dvoch úrovní jazyka. Aby sa zamedzilo tomuto konfliktu, axiomatické teórie množín sú postavené na použití dvoch rôznych jazykov. Jazyk, pomocou ktorého sa o týchto teóriách hovorí, sa nazýva **metajazyk** a jazyk, v ktorom sú vytvorené objekty danej teórie je tzv. **objektový jazyk**. Komplikácie, ktorých pôvodom bolo objavenie ďalších paradoxov, zasiahli vo svojich dôsledkoch matematiku ako celok. To viedlo k precíznemu preskúmaniu matematiky od jej základov a prispelo k rozvoji matematickej logiky a teórie množín. Podieľalo sa na tom mnoho matematikov a ich niekoľkoročné snaženie vyústilo k prijatiu axiomatickej metódy, vďaka ktorej nastal aktívny rozmach mnohých ďalších matematických disciplín. Princíp tejto metódy spočíva v tom, že na základe presne zadefinovaných axiómov sa postupne buduje množinové univerzum, ktoré podlieha určitým obmedzeniam.

Najrozšírenejšou a najdôležitejšou axiomatickou teóriou je **Zermelo-Fraenkelova teória množín**, ďalšími známymi sú **Gödel-Bernaysova teória množín** a trochu menej známa **Kelley-Morseova teória množín**.

Túto kapitolu sme spracovali s pomocou zdrojov [8], [7].

[2] Definovanie prvkov množiny na ňu samotnú.

4 Prehľad jednotlivých axiomatických teórií množín

4.1 Zermelo-Fraenkelová teória množín

Ako bolo spomenuté, táto teória je najhlavnejšou axiomatickou teóriou a budeme ju označovať skratkou ZF. Patrí medzi teórie s rovnosťou. Jej axiómy musia zaručiť hlavne dostatočne veľké univerzum a súčasne musia z neho vylúčiť také zoskupenia množín, ktoré v Cantorovej teórií viedli k paradoxom. To je dôvod, prečo sa väčšina axiómov tejto teórie zaoberá práve existenciou množín.

Axiómy tejto teórie sú:

- **Axióm existencie množín**
  Tento axióm zaručuje, že existuje aspoň jedna množina, teda že univerzum množín nie je prázdne. Tento axióm vychádza z axiómu nekonečna, ktorému sa budeme venovať neskôr. Spomenutý axióm nekonečna niektoré ďalšie časti axiomatickej teórie množín neobsahujú, preto je v nich axióm existencie množín nevyhnutný.

  $(\exists x)(x = x)$

- **Axióm extenzionality**
  Axióm popisuje vzťah medzi predikátmi náležania a rovnosti. Vyplýva z neho tvrdenie, že ak majú dve množiny rovnaké prvky, tak sa rovnajú. Z faktu, že základnými objektami axiomatickej teórie množín sú množiny, vyplýva, že prvkami množín môžu byť ďalšie množiny a nič iné. Predikát rovnosti tu má všeobecné vlastnosti stanovené axiómom rovnosti v matematickej logike.

  $(\forall u)(u \in x \leftrightarrow u \in y) \rightarrow x = y$

- **Axióm vydelenia - schéma**
  Z každej množiny možno vyčleniť množinu prvkov, ktoré spĺňajú danú formulu. Nasledujúca formula je axiómom vydelenia, ak formula $\varphi(x)$ neobsahuje voľnú premennú z.

  $(\forall a)(\exists z)(\forall x)(x \in z \leftrightarrow (x \in a \wedge \varphi(x)))$

  Pojem schéma je tu zavedený kvôli tomu, že pre konkrétne zadefinovanú formulu $\varphi(x)$ dostaneme konkrétny axióm vydelenia, čiže z vždy jedinečnej formule $\varphi(x)$ môžeme dostať z tejto schémy nekonečne veľa axiómov vydelenia.

- **Axióm dvojice**
  K akýmkoľvek množinám a, b možno zostrojiť množinu, ktorá obsahuje práve tieto dve množiny ako svoje prvky. Takto vzniknutá množina je jednoznačne určená pomocou axiómu extenzionality.

  $(\forall a)(\forall b)(\exists z)(\forall x)(x \in z \leftrightarrow (x = a \vee x = b))$

- **Axióm zjednotenia**
K ľubovoľnej množine a existuje množina z, ktorú tvoria množiny patriace do nejakého prvku množiny a. Definovaním množiny a je podľa axiómu extenzionality jednoznačne určená množina z.

$(\forall a)(\exists z)(\forall x)(x \in z \leftrightarrow (\exists y)(x \in y \wedge y \in a))$

- **Axióm potencie**
Každej množine je priradená množina všetkých jej podmnožín.

$(\forall a)(\exists z)(\forall x)(x \in z \leftrightarrow x \subseteq a)$

Poznámka 4.1 *Potenčná množina* množiny a je taká množina $P(a)$, ktorá je zložená zo všetkých podmnožín množiny a.
$P(a) = \{x : x \subseteq a\}$

- **Axióm nahradenia - schéma**
Axióm zaručuje, že pri definovanom zobrazení dostaneme z obrazu ľubovoľnej množiny opäť množinu.
Nasledujúca formula je axiómom nahradenia, ak formula $\psi(u, v)$ neobsahuje voľné premenné w, z.

$(\forall u)(\forall v)(\forall w)((\psi(u, v) \wedge \psi(u, w)) \rightarrow v = w) \rightarrow (\forall a)(\exists z)(\forall v)(v \in z \leftrightarrow (\exists u)(u \in a \wedge \psi(u, v)))$

Formula $\psi(u, v)$ môže mať okrem u a v aj iné voľné premenné a nahradením v za w z nej vznikne $\psi(u, w)$. Axióm nahradenia vychádza z predpokladu, že pre každé u platila formula $\psi(u, v)$ maximálne pre jednu množinu v. Ak existuje, je uvedenou formulou pridelená množine u. V druhej časti nám axióm zaručuje, že ak má ψ uvedenú vlastnosť a nahradíme prvky $u \in a$ množinami v im zodpovedajúcimi, dostaneme zase množinu. Opäť je tu použitá schéma, pretože aplikovaním $\psi(u, v)$ na formule dostaneme ďalšie axiómy nahradenia v uvedenom tvare.

- **Axióm nekonečna**
Zaručuje existenciu nekonečnej množiny.
Ak začneme množiny konštruovať od prázdnej množiny, pre ktorú platí $\varnothing \notin \varnothing$ spôsobom $x \cup \{x\} \neq x$ pokiaľ $x \notin x$ môžeme vytvárať stále ďalšie množiny, ktoré všetky budú prvkami množiny z. Existencia nekonečnej množiny vyplýva z axiómu nekonečna bez toho, aby definoval operáciu, prostredníctvom ktorej táto množina vznikne z už vzniknutých množín. Toto je dôvod, prečo sa tento axióm odlišuje od ďalších axiómov existencie množín - zjednotenia, dvojice a tým prekračuje systém obmedzenej veľkosti množín.

$(\exists z)(\varnothing \in z \wedge (\forall x)(x \in z \rightarrow x \cup \{x\} \in z))$

- **Axióm fundovanosti (regularity)**
  Pre každú neprázdnu množinu a platí, že obsahuje aspoň jeden taký prvok x, ktorý s ňou má prázdny prienik.
  Tento axióm by sa dal považovať za globálnu charakteristiku celého množinového univerza. Vylučuje z neho niektoré druhy množín, do ktorých napríklad patrí množina y, pričom by platilo $y \in y$, pretože by neexistoval prvok neprázdnej množiny $a = \{y\}$, ktorý by vyhovoval axiómu fundovanosti, keďže $y \cap \{y\} \neq \varnothing$. Axióm fundovanosti taktiež neumožňuje existenciu konečných cyklov vzťahu náležania, ktorými sú napríklad $y_1 \in y_2 \in y_1$, $y_1 \in y_2 \in y_3 \in y_1$. Taktiež o axióme fundovanosti platí, že je ekvivalentný s faktom, že iterovaním operácií potencie a zjednotenia je možné generovať univerzum množín z prázdnej množiny.

  $(\forall a)(a \neq \varnothing \rightarrow (\exists x)(x \in a \wedge x \cap a = \varnothing))$

Poznámka 4.2 Všetky predchádzajúce axiómy mali konštrukčný charakter, čiže ich zápis definuje, ako vytvárať ďalšie množiny. Avšak axióm fundovanosti alebo tiež regularity vo všeobecnosti definuje všetky možné množiny a tým popiera existenciu paradoxných množín, napríklad dvojicu množín M, N, v ktorých by platilo $M \in N \wedge N \in M$ alebo takých, ktoré by boli samy sebe prvkom.

Definovanie prázdnej množiny a operácie prieniku nám umožňuje axióm vydelenia. Axióm dvojice ponúka zavedenie jednoprvkovej množiny v tvare $\{x\}$ a operáciu zjednotenia množín je možné zaviesť z axiómu zjednotenia. Mechanizmus axiomatických teórií vychádza z toho, že vytvárajú univerzum možných množín po malých krokoch a postupne. Vytvorenie množiny zakladajú na existencii už vzniknutých množín a tento postup zaručuje, že zoskupenia prvkov, ktoré definovanými operáciami z týchto množín vzniknú, sú opäť množinami. Svojou veľkosťou nie sú takto vytvorené množiny príliš odlišné od množín, z ktorých boli odvodené. Russel v roku 1906 po analýze paradoxov špecifikoval tento princíp ako postup, pri ktorom sú zásadne obmedzené veľkosti množín.

Z axiómov zjednotenia, nekonečna, extenzionality, dvojice, potencie, zo schémy axiómu vydelenia a axiómu výberu sa skladala pôvodná Zermelova axiomatická teória množín z roku 1908. Axióm výberu sme nezadefinovali, pretože dnes obecne nepatrí medzi základné axiómy teórie množín. Ak axióm výberu nahradíme axiómom fundovanosti, dostaneme z pôvodnej Zermelovej axiomatiky Zermelovú teóriu množín. V roku 1922 bol Fraenklom doplnený axióm nahradenia. Rozšírením Zermelovej teórie množín o axióm nahradenia dostaneme štandardnú Zermelo-Fraenkelovú axiomatickú teóriu množín označovanú skratkou ZF.

Věta 4.1 *Dôsledkom niektorého axiómu nahradenia je každý axióm vydelenia.*

Důkaz. Ak je $\varphi(u)$ formulou neobsahujúcou z ako voľnú premennú, určíme v, w ako ďalšie dve premenné, pričom nie sú voľné vo formuli φ a vytvoríme formulu $\psi(u, v)$ v tvare $\varphi(u) \wedge u = v$

Potom platí

$$(\forall u)(\forall v)(\forall w)((\psi(u, v) \wedge \psi(u, w)) \rightarrow v = w)$$

a k akejkoľvek množine a existuje množina z podľa axiómu nahradenia pre formulu ψ taká, že pre každú množinu v platí vzťah

$$v \in z \rightarrow (\exists u)(u \in a \wedge \psi(u, v))$$

Zo zostrojenia formule ψ vyplýva, že je splnená pravá strana ekvivalencie práve keď $(v \in a \wedge \varphi(v))$. Pre formulu φ je tým dokázaný axióm vydelenia. ■

Věta 4.2 *Dôsledok axiómu potencie a nahradenia je axióm dvojice.*

Důkaz. Druhá potenčná množina prázdnej množiny $P(P(\varnothing))$ je tvorená práve dvomi prvkami $\varnothing$ a $\{\varnothing\}$. Ak sú a, b ľubovoľné dve množinové premenné, zkonštruujeme formulu $\psi(u, v)$

$$(u = \varnothing \wedge v = a) \vee (u = \{\varnothing\} \wedge v = b)$$

kde u, v sú dve premenné odlišné od a, b. Pre formulu $\varphi(u, v)$ platí

$$(\forall u)(\forall v)(\forall w)((\psi(u, v) \wedge \psi(u, w)) \rightarrow v = w)$$

a množina z sa skladá práve z dvoch prvkov a, b. Axióm nahradenia pre formulu ψ pridelí množine $P(P(\varnothing))$ množinu z. ■

Axiómami fundovanosti, nekonečna, nahradenia, zjednotenia, extenzionality a potencie je teda definovaná Zermelo-Fraenkelova axiomatická teória množín. Z týchto axiómov je vyvoditeľný axióm dvojice a každý axióm vydelenia je dôsledkom niektorého axiómu nahradenia.

4.2 Gödel-Bernaysova teória množín

Budeme ju označovať skratkou GB. Jazyk Gödel-Bernaysovej teórie množín pracuje tiež len s jediným predikátom $\in$ a s jedným druhom premenných značených veľkými písmenami, ktoré sa nazývajú *triedne premenné*. Táto teória je tiež teóriou s rovnosťou. Formula, ktorá neobsahuje kvantifikátory viazané na triedne premenné, sa nazýva *normálna formula*. Túto teóriu tvoria nasledujúce axiómy, v ktorých sú malými písmenami značené množinové premenné.

- **Axióm existencie množiny**
  $(\exists x, y)(x \in y)$

- **Axióm zavedenia množinových premenných**
  $(\exists x)(x = X) \equiv (\exists Y)(X \in Y)$

- **Axióm extenzionality pre triedy**
  $(\forall X, Y)[X = Y \equiv (\forall e)(e \in X \equiv e \in Y)]$

- **Axióm existencie tried - schéma**, ktorý platí za predpokladu, že Φ je definovaná ako *normálna* formula s nevyskytujúcou sa premennou Z.
  $(\exists Z)(\forall e)(e \in Z \equiv \Phi)$

- **Axióm dvojice**
  $(\forall x, y)(\exists z)(\forall e)[e \in z \equiv (e = x \vee e = y)]$

- **Axióm nahradenia**
  $(\forall F)((\forall y, e_1, e_2)[(\langle e_1, y\rangle \in F \wedge \langle e_2, y\rangle \in F) \rightarrow e_1 = e_2] \rightarrow (\forall x)(\exists z)(\forall e)[e \in z \equiv (\exists y)(y \in x \wedge \langle e, y\rangle \in F)])$

a **Axiómy potencie, fundovanosti, nekonečna a zjednotenia**, ktoré sú s množinovými premennými a presne v tvare definovanom v ZF teórií.

4.3 Kelley-Morseova teória množín

Na označenie budeme používať skratku KM. Táto teória je od predchádzajúcej odlišná v jedinej veci, a to vo vynechaní slova *normálna* v definícií axiómu existencie tried. Význam to mení v tom, že je požadovaná existencia tried pre všetky formule, ktoré splňujú požiadavku na voľnosť premenných. Platí to aj pre formule, ktoré obsahujú kvantifikátory triednych premenných. Takto zkonštruovanú schému axiómu existencie tried nie je možné nahradiť konečným počtom jeho prípadov a táto schéma umožňuje len existenciu triedy množín s danou vlastnosťou, čiže ak by sme napríklad vyžadovali existenciu triedy tried X s vlastnosťou Φ pre každú formulu $\Phi(X)$, pri správne zadefinovaj formuli Φ by sme dospeli ku sporu.

K spracovaniu tejto kapitoly nám pomohli zdroje [1], [2].

5 Porovnanie vybraných teórií množín

Na začiatok uvedieme a zadefinujeme niektoré pojmy, s ktorými budeme neskôr pracovať.

Neusporiadaná dvojica je definovaná vzťahom: $z = \{x, y\} \equiv (\forall e)[e \in z \equiv (e = x \vee e = y)]$. Táto definícia konzervatívne rozširuje teóriu ZF. Dôkazom toho je platnosť formule $ZF \vdash (\forall x, y)(\exists! z)(\forall e)[e \in z \equiv (e = x \vee e = y)]$, na ktorú potom stačí už len použiť vetu o definícii funkcie. Na dôkaz jednoznačnosti formule $(\forall x, y)(\exists z)(\forall e)[e \in z \equiv (e = x \vee e = y)]$ stačí aplikovať axióm extenzionality tak, že je pre každé x a y treba preukázať $(\forall z_1, z_2)[((\forall e)[e \in z_1 \equiv (e = x \vee e = y)] \wedge (\forall e)[e \in z_2 \equiv (e = x \vee e = y)]) \rightarrow z_1 = z_2]$. Použitie definície $z = \{x, y\} \equiv (\forall e)[e \in z \equiv (e = x \vee e = y)]$ nie je možné v teóriách množín s triedami, pretože funkcia musí byť definovaná aj pre vlastné triedy, teda pre všetky objekty. Kvôli tomu sa uvedená formula upravuje na $z = \{X, Y\} \equiv (\forall e)[e \in z \equiv (e = X \vee e = Y)]$, pričom musí byť splnené, aby hodnota X, Y bola množinou pre akékoľvek objekty X, Y. Z toho vyplýva, už je pre akúkoľvek dvojicu objektov funkcia definovaná, keďže jednoznačnosť formule $(\forall X, Y)(\exists! z)(\forall e)[e \in z \equiv (e = X \vee e = Y)]$ je dôsledkom axiómu extenzionality a axiómu dvojice. Axióm dvojice sa síce zaoberá len množinami, ale v konkrétnom prípade toto obmedzenie nie je na úkor všeobecnosti, keďže požadujeme, aby prvkom dvojice $\{X, Y\}$ bola trieda X a/alebo trieda Y, práve keď je množinou. Keďže je v teórií GB dokázateľná formula $\neg(\forall X, y)(X \in \{X, y\})$, pri použití takto definovanej funkcie musíme dbať na zvýšenú opatrnosť. Náležanie do dvojice je dokázateľné iba pre množiny, napríklad $GB \vdash (\forall x, Y)(x \in \{x, Y\})$.

Usporiadaná dvojica je v ZF definovaná formulou $z = \langle x, y\rangle \equiv z = \{\{x\}, \{x, y\}\}$ a v GB a KM teóriách množín $Z = \langle X, Y\rangle \equiv Z = \{\{X\}, \{X, Y\}\}$, pričom $\{x\}$ a $\{X\}$ je skrátená forma $\{x, x\}$ a $\{X, X\}$. Formula $\langle x_1, y_1\rangle = \langle x_2, y_2\rangle \rightarrow (x_1 = x_2 \wedge y_1 = y_2)$ je dokázateľná v ZF teórií, ale musíme dávať pozor v teóriách množín pracujúcimi s triedami, pretože formula vypovedajúca aj o vlastných triedach $\langle X_1, Y_1\rangle = \langle X_2, Y_2\rangle \rightarrow (X_1 = X_2 \wedge Y_1 = Y_2)$ už nie je dokázateľná ani v KM, keďže je $\langle X_1, Y_1\rangle = \{\varnothing\} = \langle X_2, Y_2\rangle$ pre akékoľvek vlastné triedy X_1, X_2, Y_1, Y_2.

Usporiadaná k-tica ($k > 2$**)** je v ZF definovaná formulou $z = \langle x_1, x_2, ..., x_k\rangle \equiv z = \langle x_1\langle x_2, ..., x_k\rangle\rangle$ a v GB a KM formulou $Z = \langle X_1, X_2, ..., X_k\rangle \equiv Z = \langle X_1\langle X_2, ..., X_k\rangle\rangle$. Ak $k = 1$ v ZF platí $z = \langle x\rangle \equiv z = x$ a v teóriách s triedami $Z = \langle X\rangle \equiv Z = X$.

Ak je relácia r na množine m reflexívna, tranzitívna a slabo antisymetrická (ak $\langle x, y\rangle$ aj $\langle y, x\rangle$ sú prvkami, tak platí $x = y$), tak je **usporiadaním**. Ak v takejto množine m má každá jej neprázdna podmnožina najmenší prvok, tak je toto usporiadanie **dobré**.

Dve množiny (triedy) x, y nazývame **izomorfnými** vzhľadom k reláciám r, s, ak existuje prostá funkcia f, pre ktorú platí $Dom(f) = x \wedge Rng(f) = y \wedge (\forall e_1, e_2 \in x)(\langle e_1, e_2\rangle \in r \equiv \langle f(e_1), f(e_2)\rangle \in s)$. Takúto funkciu nazývame izomorfizmus. Symbol $Dom(f)$ definuje funkciu definičného oboru, všeobecný zápis je $z = Dom(x) \equiv (\forall e)[e \in z \equiv (\exists y)(\langle y, e\rangle \in x)]$, kde z reprezentuje množinovú premennú a symbol Rng zastupuje funkciu oboru hodnôt definovanú $z = Rng(x) \equiv (\forall e)[e \in z \equiv (\exists y)(\langle e, y\rangle \in x)]$

Stanovme, že množina m je reláciou r usporiadaná tým istým typom, ako množina n reláciou s, ak sú relačné štruktúry $\langle m, r\rangle$, $\langle n, s\rangle$ izomorfné. Typ usporiadania r množiny m je teda definovaný len samotným usporiadaním, nie je ovplyvnený prvkami množiny m a vzťahmi medzi nimi, okrem vzťahu definovaného reláciou r. Ak extrahujeme z dobrého usporiadania nejakej množiny samotný typ tohto usporiadania, tak tento typ reprezentujeme ako **ordinálne číslo**. Pomocou axiómu $Ord(x) \equiv (\forall e_1, e_2 \in x)[e_1 \subseteq x \wedge (e_1 \in e_2 \vee e_1 = e_2 \vee e_2 \in e_1)]$ sa v ZF teórií množín definuje unárny predikát „byť ordinálnym číslom" (Ord). Symbolom On je označená trieda ordinálnych čísel. Prijímame axióm, ktorý definuje nový druh premenných tvaru $(\exists \alpha)(\alpha = x) \equiv Ord(x)$, keďže premenné α, β, γ budú prechádzať ordinálne čísla.

Reláciou $\underline{\in}$ je dobre usporiadaný systém ordinálnych čísel, keďže platí $(\forall x)([(\exists e)(e \in x) \wedge (\forall e \in x)Ord(e)] \rightarrow (\exists e \in x)(\forall z \in x)(z \notin e))$. Pre každé ordinálne číslo α je množina $\alpha \cup \{\alpha\}$ nasledovníkom čísla α. Dosiahneme to aplikáciou definície ordinálneho čísla, teda $Ord(\alpha \cup \{\alpha\}) \wedge \neg(\exists y)(\alpha \in y \in \alpha \cup \{\alpha\})$. Označenie $\alpha + 1$ označuje nasledovníka ordinálneho čísla α, pričom následníka $\varnothing$, teda množinu $\{\varnothing\}$ označuje 1.

Množina x, ktorá je dobre usporiadaná usporiadaním $\leq$, tak je vzhľadom k usporiadaniu $\leq$ a $\underline{\in}$ izomorfná práve jednému ordinálnemu číslu. Ak neexistuje vzájomne jednoznačné zobrazenie ordinálneho čísla α na nejaké $\beta \in \alpha$, nazýva sa toto ordinálne číslo **kardinálnym**. Pre každú množinu x, ktorú je možné dobre usporiadať, existuje práve jedno kardinálne číslo k, pričom platí, že existuje vzájomne jednoznačné zobrazenie x na k. Potom sa toto kardinálne číslo k nazýva *mohutnosťou* množiny x. Definujme, že funkcie $+$ a $.$ priraďujú ordinálny súčet a súčin ordinálnym číslam a konštantu $\varnothing$ ostatným množinám. Potom $\alpha + \beta$ je to jediné ordinálne číslo, ktoré je množine $(\{\varnothing\} \times \alpha) \cup (\{1\} \times \beta)$ vzhľadom k usporiadaniu $\underline{\in}$ a lexikografickému usporiadaniu dvojíc vzniknutých z usporiadania $\underline{\in}$, izomorfné. Taktiež $\alpha.\beta$ je to jediné ordinálne číslo, ktoré je množine $\beta \times \alpha$ vzhľadom k usporiadaniu $\underline{\in}$ a lexikografickému usporiadaniu dvojíc vzniknutých z usporiadania $\underline{\in}$, izomorfné. Prirodzené čísla môžeme v ZF a GB teórií definovať ako tie ordinálne čísla, ktoré sú konečnými množinami. Označením $m, n, ...$ budeme značiť takto získaný nový druh premenných, ktoré pridaním axiómu $(\exists m)(x = m) \equiv [Ord(x) \wedge Fin(x)]$ získame. Unárny predikát $Fin(x)$ značí vlastnosť „byť konečnou triedou" a je definovaný formulou $Fin(X) \equiv (\forall y \subseteq P(X))(y \neq \varnothing \rightarrow (\exists z)[z \in y \wedge (\forall e \in y)\neg(z \subseteq e \wedge z \neq e)])$, pričom P symbolizuje potenciu triedy, ktorá je definovaná $Z = P(X) \equiv (\forall e)[e \in Z \equiv (\forall y)(y \in e \rightarrow y \in X)]$.

Spĺňanie v štruktúre U v jazyku teórie množín vo všeobecnosti tvoria množiny U a R. R je množina niektorých usporiadaných dvojíc prvkov, pričom je táto dvojica prvkom množiny U, takže je R reláciou na množine U. Množinu U nazývame univerzom štruktúry a jej prvky sú individuá. **Ohodnotenie v štruktúre** U je konečné zobrazenie, ktoré priraďuje niektorým premenným prvky univerza U. Ohodnotenie definujeme ako $e(x \longmapsto a)$, ak je e ohodnotenie v štruktúre U a a je individuum, čiže je to funkcia, ktorá na všetkých premenných okrem x nadobúda rovnaké hodnoty, ako e a pre premennú x nadobúda hodnotu a. Napríklad značenie $x_1 \longmapsto a_1, ..., x_k \longmapsto a_k$ (=$e(x_1 \longmapsto a_1, ..., x_k \longmapsto a_k)$, kde e je prázdnou funkciou) reprezentuje ohodnotenie, ktoré po rade priraďuje premenným $x_1, ..., x_k$ individuá $a_1, ..., a_k$. Definujme, že U je štruktúra v jazyku teórie množín, formulou tohto jazyka je α a e je ohodnotenie v U, ktoré je zadefinované vo formuli α na množine všetkých jej voľných premenných. Ak je e definované pre všetky premenné potrebné v zápisoch na pravých stranách nasledujúcich ekvivalencií, indukciou podľa zložitosti formule α zadefinujeme ternárny vzťah $U \models \alpha[e]$ nasledovne:

- $U \models (x = n)[e] \equiv e(x) = e(n)$
  (rovnosť v štruktúre je faktickou rovnosťou)
- $U \models (x \in n)[e] \equiv \langle e(x), e(n) \rangle \in R$
  ($x \in n$ sú voľné premenné x a n, pričom je pre tieto argumenty e definované; hodnoty $e(x)$ a $e(n)$ sú individuá štruktúry U)
- $U \models (\neg\beta)[e] \equiv$ neexistuje $U \models \beta[e]$
- $U \models (\beta \wedge \gamma)[e] \equiv (U \models \beta[e] \wedge U \models \gamma[e])$
- $U \models ((\exists x)\alpha)[e] \equiv$ existuje také $a \in U$ individuum, že $U \models \alpha[e(x \longmapsto a)]$

Formula α je pri ohodnotení e pravdivá v štruktúre U tvrdíme, ak platí zápis $U \models \alpha[e]$. Ak pri každom ohodnotení v štruktúre U je α pravdivá, tak tvrdíme, že je formula α splnená v štruktúre U a zapisujeme $U \models \alpha$. Ak je v takejto štruktúre splnený každý axióm nejakej teórie T, tak je táto štruktúra *modelom teórie* T. Každá štruktúra, v ktorej je absencia mimologických axiómov, je modelom teórie. Ak vo formuli $\alpha(x_1, ..., x_k)$ vyznačíme všetky jej voľné premenné a ich poradie dopredu, napríklad formou zápisu, tak budú pre každú štruktúru U v jazyku teórie množín a pre akékoľvek jej individuá $a_1, ..., a_k$ vyjadrovať zápisy $U \models \alpha[x_1 \longmapsto a_1, ..., x_k \longmapsto a_k]$ a $U \models \alpha[a_1, ..., a_k]$ to isté. Pre akékoľvek individuá a, b a pre konkrétnu formulu $x \in n$ v štruktúre U bude význam zápisov $U \models x \in n[a, b]$ a $U \models a \in b$ totožný.

Pre každú normálnu formulu Φ, ktorá neobsahuje premennú Z, je bežným pridanie novej funkcie $\{\tilde{e}; \Phi(e/\tilde{e})\}$ zadefinovaním pomocou $Z = \{\tilde{e}; \Phi(e/\tilde{e})\} \equiv (\forall e)(e \in Z \equiv \Phi)$ v teóriách množín GB a KM. Zadefinovanie takejto funkcie je založené na základe extenzionality pre triedy, axiómu existencie tried vzniknutého zo schémy štvrtého axiómu GB axiomatického systému aplikovaného na formulu Φ a využitím vety o definícií funkcie.

Keďže axiomatický systém ZF teórie množín obsahuje konečne veľa axiómov, je možné tvrdiť, že je rekurzívny. To znamená, že existuje pre takúto teóriu algoritmus, ktorý o akejkoľvek formuli dokáže rozhodnúť, či je alebo nie je axiómom. Z druhej Gödelovej vety o neúplnosti (ktorá popisuje, že ak je nejaká teória T bezosporná a rekurzívna, pričom je rozšírením Peanovej aritmetiky (sú v nej dokázateľné všetky axiómy Peanovej aritmetiky), potom formulu $Con(T)$, ktorá vyjadruje neexistenciu formálneho dôkazu sporu vo formálnej teórie T, nie je možné dokázať v T) vyplýva, že formula $Con(ZF)$ je za predpokladu bezospornosti teórie ZF nedokázateľná v teórií ZF. Našou úlohou teda bude preukázať, že $Con(ZF)$ je dokázateľná v teórií KM. Uskutočníme to demonštráciou na konkrétnej formuli, ktorú bude možné v jednej teórií dokázať a v druhej nie. Automaticky tak stanovíme silu jednotlivých teórií.

Keďže vo formuli $Con(ZF)$ predpokladáme nielen predikáty $=$ a $\in$, ale napríklad aj pojmy „byť formálnou formulou formálneho jazyka", „byť formálnym dôkazom vo formálnej teórií" alebo „byť prirodzeným číslom", nemôžeme takúto formulu považovať za riadnu formulu jazyka teórie množín. Týmito pojmami sme rozšírili nielen jazyk teórie ZF, ale definíciami predikátov, funkcií a druhov premenných aj jeho axiomatický systém. Už vieme, že konzervatívnym rozšírením teórie ZF je takto vzniknutá teória ZF′, pričom k formuli ψ pôvodného jazyka existuje formula rozšíreného jazyka φ. Takže existuje taká formula ψ jazyka teórie množín k formuli $Con(ZF)$, že platí $ZF' \vdash Con(ZF) \equiv \psi$. V teórií ZF′ je dokázateľné, že formálna teória ZF′ je formálnym konzervatívnym rozšírením formálnej teórie ZF, platí $ZF' \vdash Con(ZF) \equiv Con(ZF')$.

Vlastnú triedu všetkých konečných funkcií označených v zobrazujúcich časť množiny označenej Var do univerzálnej triedy označenej V označíme Ev. Ak platí $v \in Ev$, označíme ohodnotenie, ktoré je totožné s ohodnotením v na všetkých formálnych premenných okrem premennej x, kde nadobúda hodnoty x, znakom $v(x \longmapsto x)$ (kde $x \longmapsto x$ symbolizuje ohodnotenie, teda priradenie indivituí k voľným premenným), teda v symboloch $v \restriction (Var - \{x\}) = v(x \longmapsto x) \restriction (Var - \{x\}) \wedge v(x \longmapsto x)(x) = x$. Symbol $\restriction$ vyjadruje funkciu reštrikcie, ktorá je všeobecne definovaná formulou $Z = X \restriction Y \equiv (\forall e)[e \in Z \equiv (\exists x, y)(e = \langle x, y\rangle \wedge e \in X \wedge y \in Y)]$. Budeme sa zaoberať zadefinovaním binárneho predikátu tak, aby v štruktúre, ktorej univerzom je trieda V a v nej je predikát náležania definovaný faktickým náležaním, bola pri ohodnotení v formálna formula π pravdivá a bolo to vyjadrené formulou $V \models \pi[v]$. Ohodnotenie v je definované minimálne pre všetky voľné premenné formúl na pravej strane v nasledujúcich ekvivalenciách. Naším cieľom je, aby platilo pre akékoľvek formálne formule π, ϱ, pre akékoľvek formálne premenné x, y a pre ľubovoľné ohodnotenie v platilo:

$V \models x \in y[v] \equiv v(x) \in v(y)$; $V \models x = y[v] \equiv v(x) = v(y)$;
$V \models (\pi \wedge \varrho)[v] \equiv (V \models \pi[v] \wedge V \models \varrho[v])$; $V \models \neg\pi[v] \equiv \neg(V \models \pi[v])$;
$V \models (\exists x)\pi[v] \equiv (\exists x)(V \models \pi[v(x \longmapsto x)])$

Postupné zadefinovanie predikátu podľa zložitosti formule π nám definícia zavedenia predikátu neumožňuje, pretože indukcia podľa zložitosti formule, ktorej krokmi by boli vyššie uvedené zadefinované požiadavky nám správnosť zadefinovania predikátu negarantuje. Pritom ale v KM teórií je dokázateľná existencia takej relácie Sat, že zadefinovaním $V \models \pi[v] \equiv \langle v, \pi\rangle \in Sat$ získame predikát, ktorý už bude tieto požiadavky spĺňať. Správnou voľbou vlastnosti Φ dokážeme existenciu takejto relácie Sat. Požiadavou na túto vlastnosť je, že by jej mali vyhovovať parcializácie konštrukcie relácie Sat na triedy formálnych formulí, ktoré sú uzavreté na podformule obsahujúce formule tvarov $x \in y$ a $x = y$. Reláciu Sat budeme zostrojovať v KM teórií množín a v GB teórií zkonštruujeme formulu Φ, ktorá bude reprezentovaná ako $\Phi(R, X)$ a zadefinovaná nasledovne:

$$Dom(R) \subseteq X \subseteq Form \wedge Rng(R) \subseteq Ev \wedge (\forall v \in Ev)((\forall x, y \in Var)([\langle v, x \in y\rangle \in R \equiv (\{x,y\} \subseteq Dom(v) \wedge v(x) \in v(y))] \wedge [\langle v, x = y\rangle \in R \equiv (\{x,y\} \subseteq Dom(v) \wedge v(x) = v(y))]) \wedge (\forall \pi, \varrho \in Form)[(\pi \wedge \varrho \in X \rightarrow [\langle v, \pi \wedge \varrho\rangle \in R \equiv (\langle v, \pi\rangle \in R \wedge \langle v, \varrho\rangle \in R)]) \wedge (\neg\pi \in X \rightarrow [\langle v, \neg\pi\rangle \in R \equiv (\langle v, \pi\rangle \notin R \wedge Free(\pi) \subseteq Dom(v))]) \wedge (\forall x \in Var)((\exists x)\pi \in X \rightarrow [\langle v, (\exists x)\pi\rangle \in R \equiv (\exists x)(\langle v(x \longmapsto x), \pi\rangle \in R)]) \wedge [(Sf(\pi, \varrho) \wedge \varrho \in X) \rightarrow \pi \in X]]),$$

kde $Form$ symbolizuje množinu formálnych formulí, $Free(\pi)$ značí množinu formálnych voľných premenných formálnej formule π a Sf je binárnym predikátom, pričom formula $Sf(\pi, \varrho)$ vyjadruje, že formálna formula π je formálnou podformulou formule ϱ.

Medzi formulou $(\exists x)\pi$ a práve tými ohodnoteniami v, pre ktoré existuje ohodnotenie, ktoré je vo vzťahu s π a je zhodné s v všade možno okrem formálnej premennej x, vytvoríme vzťah. Tento krok bude symbolizovať existenčnú kvantifikáciu. Inklúzia $Free(\pi) \subseteq Dom(v)$ v zadefinovaní formule Φ je zaručená len pre tie formule π, ktoré sú základnými formulami alebo negáciami. Nasledujúcu implikáciu $(\Phi(R, X) \wedge \langle v, \pi\rangle \in R) \rightarrow Free(\pi) \subseteq Dom(v)$ dokážeme pre ľubovoľnú formulu π a každé $v \in Ev$ indukciou. Žiadané vlastnosti formule Φ musíme rozšíriť vhodným spôsobom, ak chápeme ako samostatné operácie ekvivalenciu, univerzálnu kvantifikáciu, implikáciu a disjunkciu. To znamená, že ak ich chápeme ako skratky formálnych formulí interpretovaných iba konjunkciou, negáciou a existenčnou kvantifikáciou. Ak predpokladáme $\Phi(R, X)$ a ak sú prvkami triedy X spomínané formule, získame nasledujúce vzťahy:

$$\langle v, \pi \rightarrow \varrho\rangle \in R \equiv \langle v, \neg(\pi \wedge \neg\varrho)\rangle \in R$$

$$\langle v, \pi \rightarrow \varrho\rangle \in R \equiv [\neg(\langle v, \pi\rangle \in R \wedge \langle v, \varrho\rangle \notin R) \wedge Free(\pi \wedge \neg\varrho) \subseteq Dom(v)]$$

$$\langle v, \pi \rightarrow \varrho\rangle \in R \equiv [(\langle v, \pi\rangle \in R \rightarrow \langle v, \varrho\rangle \in R) \wedge Free(\pi \rightarrow \varrho) \subseteq Dom(v)]$$

$$\langle v, \pi \vee \varrho\rangle \in R \equiv \langle v, \neg(\neg\pi \wedge \neg\varrho)\rangle \in R$$

$$\langle v, \pi \vee \varrho\rangle \in R \equiv [\neg(\langle v, \pi\rangle \notin R \wedge \langle v, \varrho\rangle \notin R) \wedge Free(\neg\pi \wedge \neg\varrho) \subseteq Dom(v)]$$

$$\langle v, \pi \vee \varrho\rangle \in R \equiv [(\langle v, \pi\rangle \in R \vee \langle v, \pi\rangle \in R) \wedge Free(\pi \vee \varrho) \subseteq Dom(v)]$$

$$\langle v, \pi \equiv \varrho\rangle \in R \equiv (\langle v, (\pi \rightarrow \varrho) \wedge (\varrho \rightarrow \pi)\rangle \in R)$$

$$\langle v, \pi \equiv \varrho\rangle \in R \equiv [(\langle v, \pi\rangle \in R \equiv \langle v, \varrho\rangle \in R) \wedge Free(\pi \equiv \varrho) \subseteq Dom(v)]$$

$\langle v, (\forall x)\pi\rangle \in R \equiv \langle v, \neg(\exists x)\neg\pi\rangle \in R$

$\langle v, (\forall x)\pi\rangle \in R \equiv [\neg(\exists x)(\langle v(x \longmapsto x), \neg\pi\rangle \in R) \wedge Free((\exists x)\neg\pi) \subseteq Dom(v)]$

$\langle v, (\forall x)\pi\rangle \in R \equiv [(\forall x)(\langle v(x \longmapsto x), \pi\rangle \in R)]$

Platí vzťah $\Phi(R, X) \to \Phi(R \restriction Y, Y)$, ak platí, že je trieda $Y \subseteq X$ uzavretá na podformule a obsahuje atomické formule.

Věta 5.1 *Ak v GB teórií množín uvažujeme $\Phi(R, X) \wedge \Phi(S, X)$, vyplýva z toho $R = S$.*

Důkaz. Toto tvrdenie dokážeme indukciou. Tým, že kód podpostupnosti je pri bežnom usporiadaní prirodzených čísel menší, ako kód postupnosti, je možné zkonštruovať kódovanie konečných postupností prirodzených čísel. Z toho vyplýva, že kód podformule, je menší, ako kód formule. $\{\pi \in X; (\exists v \in Ev)\neg(\langle v, \pi\rangle \in R \equiv \langle v, \pi\rangle \in S)\}$ je existujúcou triedou a je aj množinou. Platí, že by bolo možné fixovať jej najmenší prvok π, ak by bola neprázdna. π je v takom prípade existenčnou kvantifikáciou alebo formálnou konjunkciou alebo negáciou nejakej svojej formálnej podformule/podformulí. Prvkom triedy X je každá podformula ϱ formule π. Inklúzia $Free(\pi) \subseteq Dom(v)$ nie je závislá na reláciach R, S, takže pre takúto podformulu ϱ platí $\langle v, \pi\rangle \in R \equiv \langle v, \pi\rangle \in S$. ∎

Hodnoty ohodnotenia v na voľných premenných formálnej formule π rozhodujú o tom, či je prvkom R dvojica $\langle v, \pi\rangle$. Použijeme na to indukciu. Ak sú v_1, v_2 dve ohodnotenia, potom platí **(1)** $[\Phi(R, X) \wedge \pi \in X \wedge (\forall x \in Free(\pi))(v_1(x) = v_2(x))] \to (\langle v_1, \pi\rangle \in R \equiv \langle v_2, \pi\rangle \in R)$. V nasledujúcej vete je tvrdené, že ak je možné reláciu splňovania zadefinovať pre formule π, ϱ, tak je aj pre formule $\pi \wedge \varrho$ a $\neg\pi$ možné túto reláciu zadefinovať taktiež. A pri predpoklade, že x je formálnou premennou, aj pre formulu $(\exists x)\pi$.

Věta 5.2 *Ak platí $\pi \in X \wedge \Phi(R, X)$, $\varrho \in Y \wedge \Phi(S, Y)$ a ak je x formálna premenná, tak existuje Q, Z také, že platí $X \cup Y \subseteq Z \wedge \pi \wedge \varrho \in Z \wedge \neg\pi \in Z \wedge (\exists x)\pi \in Z \wedge \Phi(Q, Z)$.*

Důkaz. Pre určené triedy R, S, X, Y v GB teórií definujeme

$Z = X \cup Y \cup \{\pi \wedge \varrho\} \cup \{\neg\pi\} \cup \{(\exists x)\pi\}$

$Q = R \cup S \cup \{\langle v, \pi \wedge \varrho\rangle; \langle v, \pi\rangle \in R \wedge \langle v, \varrho\rangle \in S\} \cup \{\langle v, \neg\pi\rangle; v \in Ev \wedge \langle v, \pi\rangle \notin R \wedge Free(\pi) \subseteq Dom(v)\} \cup \{\langle v, (\exists x)\pi\rangle; (\exists x)(\langle v(x \longmapsto x), \pi\rangle \in R)\}$

Keďže platí $\pi \in X \wedge \varrho \in Y$, tak je trieda Z uzavretá na podformule svojích prvkov. V dôsledku predchádzajúceho dôkazu získame $\Phi(Q, Z)$ pomocou overenia definície formule Φ. ∎

Věta 5.3 *V GB teórií je dokázateľné $(\Phi(R, X) \wedge \varphi \in X) \to (\forall v \in Ev)(\varphi(x_1, ..., x_n) \equiv \langle v(x_1 \longmapsto x_1, ..., x_n \longmapsto x_n), \varphi\rangle \in R)$ pre každú množinovú formulu $\varphi(x_1, ..., x_n)$.*

Důkaz. Pri predpoklade $\Phi(R, X)$ získame indukciou podľa zložitosti formule φ a pomocou definíc základné formule:

$x \in y \equiv \langle v(x \longmapsto x, y \longmapsto y), x \in y\rangle \in R \equiv v(x \longmapsto x, y \longmapsto y)(x) \in v(x \longmapsto x, y \longmapsto y)(y)$

$x = y \equiv \langle v(x \longmapsto x, y \longmapsto y), x = y\rangle \in R \equiv v(x \longmapsto x, y \longmapsto y)(x) = v(x \longmapsto x, y \longmapsto y)(y)$

Budeme predpokladať $\Phi(R, X) \wedge \varphi \wedge \psi \in X$ a pričom ako dve množinové formule zadefinujeme $\varphi(x_1, ..., x_n)$ a $\psi(y_1, ..., y_m)$. Potom platí $\varphi \in X \wedge \psi \in X$. Premenné, ktoré sú v postupnosti $y_1, ..., y_m$ a súčastne nie sú v postupnosti $x_1, ..., x_n$, označíme ako $y'_1, ..., y'_{m'}$. Potom sú všetky voľné premenné formule $\varphi \wedge \psi$ medzi premennými $x_1, ..., x_n, y'_1, ..., y'_{m'}$ a podľa indukčného predpokladu platí $(\varphi \wedge \psi)(x_1, ..., x_n, y'_1, ..., y'_{m'}) \equiv (\langle v(x_1 \longmapsto x_1, ..., x_n \longmapsto x_n, y'_1 \longmapsto y'_1, ..., y'_{m'} \longmapsto y'_{m'}), \varphi\rangle \in R \wedge \langle v(x_1 \longmapsto x_1, ..., x_n \longmapsto x_n, y'_1 \longmapsto y'_1, ..., y'_{m'} \longmapsto y'_{m'}), \psi\rangle \in R)$.

Ak dokážeme $\langle v(x_1 \longmapsto x_1, ..., x_n \longmapsto x_n, y'_1 \longmapsto y'_1, ..., y'_{m'} \longmapsto y'_{m'}), \varphi\rangle \in R \equiv \langle v(x_1 \longmapsto x_1, ..., x_n \longmapsto x_n), \varphi\rangle \in R$, takmer dokončíme dokazovanie skúmaného indukčného kroku. Formálne premenné $y'_1, ..., y'_{m'}$ nie sú formálnymi voľnými premennými formálnej formule φ, keďže premenné $y'_1, ..., y'_{m'}$ nie sú voľnými premennými formule φ, takže stačí použiť vzťah (1) uvedený v dôkaze Vety 1.

Rovnaký postup uplatníme aj pre formulu ψ: Ak platí $\Phi(R, X) \wedge \neg\varphi \in X$, tak $\varphi \in X$, tak nám indukčný predpoklad zaistí $\neg\varphi(x_1, ..., x_n) \equiv \neg\langle v(x_1 \longmapsto x_1, ..., x_n \longmapsto x_n), \varphi\rangle \in R \equiv \langle v(x_1 \longmapsto x_1, ..., x_n \longmapsto x_n), \neg\varphi\rangle \in R$. Predpokladajme $\Phi(R, X) \wedge (\exists x)\varphi \in X$, pričom $\varphi(x, x_1, ..., x_n)$ je ľubovoľná formula definujúca množinu. Potom platí $\varphi \in X$ a pre všetky rôzne premenné $x, x_1, ..., x_n$ a pre každé ohodnotenie v platí $v(x \longmapsto x, x_1 \longmapsto x_1, ..., x_n \longmapsto x_n) = (v(x_1 \longmapsto x_1, ..., x_n \longmapsto x_n))(x \longmapsto x)$. Podľa indukčného predpokladu z toho vyplýva $(\exists x)\varphi \equiv (\exists x)(\langle v(x \longmapsto x, x_1 \longmapsto x_1, ..., x_n \longmapsto x_n), \varphi\rangle \in R) \equiv (\exists x)(\langle (v(x_1 \longmapsto x_1, ..., x_n \longmapsto x_n))(x \longmapsto x), \varphi\rangle \in R) \equiv \langle v(x_1 \longmapsto x_1, ..., x_n \longmapsto x_n), (\exists x)\varphi\rangle \in R$. ■

Věta 5.4 *Pre každé triedy R, X také, že platí $\Phi(R, X) \wedge \pi \in X$, pre každú formálnu formulu π jazyka teórie množín, ktorá je v tvare axiómu logického kalkulu alebo axiómu ZF teórie množín a pre každé ohodnotenie v, ktoré je definované na všetkých formálnych voľných premenných formálnej formule π je v GB teórií množín $\langle v, \pi\rangle \in R$.*

Důkaz. Našou povinnosťou bude preukázať uvedené tvrdenie pre každý axióm samostatne, pričom jednotlivé úvahy použijeme na dokázanie tvrdení o formálnych formulách v neformalizovanej forme. Konkrétne použijeme napríklad axióm predikátového počtu typu $\alpha \to (\beta \to \alpha)$ pri skúmaní formálnej formule $\pi \to (\varrho \to \pi)$, pričom za α zadefinujeme $\langle v, \pi\rangle \in R$ a $\langle v, \varrho\rangle \in R$ za β. Predpokladajme $\Phi(R, X)$. Nech je na všetkých formálnych voľných premenných uvažovaných formulí definované $v \in Ev$ a nech prvkami triedy X sú všetky uvažované formálne formule.

Potom platí:

$\langle v, \pi \to (\varrho \to \pi)\rangle \in R \equiv [\langle v, \pi\rangle \in R \to (\langle v, \varrho\rangle \in R \to \langle v, \pi\rangle \in R)]$,

$\langle v, [\pi \to (\varrho \to \sigma)] \to [(\pi \to \varrho) \to (\pi \to \sigma)]\rangle \in R \equiv ([\langle v, \pi\rangle \in R \to (\langle v, \varrho\rangle \in R \to \langle v, \sigma\rangle \in R)] \to [(\langle v, \pi\rangle \in R \to \langle v, \varrho\rangle \in R) \to (\langle v, \pi\rangle \in R \to \langle v, \sigma\rangle \in R)])$,

$\langle v, (\neg\pi \rightarrow \neg\varrho) \rightarrow (\varrho \rightarrow \pi)\rangle \in R \equiv [(\langle v, \pi\rangle \notin R \rightarrow \langle v, \varrho\rangle \notin R) \rightarrow (\langle v, \varrho\rangle \in R \rightarrow \langle v, \pi\rangle \in R)]$.

Budeme uvažovať, že formálnu premennú y je do π možné formálne substituovať za formálnu premennú x. Potom pre S, ktoré splňuje $\Phi(S, X) \wedge \pi \in X \wedge \pi(x/y) \in X$ platí **(2)** $\langle v, \pi(x/y)\rangle \in S \equiv \langle v(x \longmapsto v(y)), \pi\rangle \in S$, pričom uvedené tvrdenie nájde uplatnenie pri skúmaní formálnych axiómov špecifikácie a dokážeme ho indukciou podľa zložitosti formálnej formule π. Pre formálnu premennú z, ktorá je buď rovná alebo rozdielna od y, platia nasledujúce vzťahy:
$\langle v, (x = z)(x/y)\rangle \in S \Leftrightarrow v(y) = v(z) \Leftrightarrow \langle v(x \longmapsto v(y)), x = z\rangle \in S$
$\langle v, (z = x)(x/y)\rangle \in S \Leftrightarrow v(z) = v(y) \Leftrightarrow \langle v(x \longmapsto v(y)), z = x\rangle \in S$
$\langle v, (x \in z)(x/y)\rangle \in S \Leftrightarrow v(y) \in v(z) \Leftrightarrow \langle v(x \longmapsto v(y)), x \in z\rangle \in S$
$\langle v, (z \in x)(x/y)\rangle \in S \Leftrightarrow v(z) \in v(y) \Leftrightarrow \langle v(x \longmapsto v(y)), z \in x\rangle \in S$

Následne sa budeme zaoberať indukčným krokom pre konjunkciu a negáciu. Predstavme si formálnu formulu $(\exists z)\varrho$, ktorej uváženie je možné v troch prípadoch. Prvé dva prípady rozoberieme len s pomocou definície Φ.

- Na začiatok budeme predpokladať, že formálna premenná x je totožná s formálnou premennou z. Je očividné, že predpokladaná formálna formula $(\exists z)\varrho$ je identická s formálnou formulou $[(\exists x)\varrho](x/y)$, keďže pri substitúcií sa nahrádzajú len voľné výskyty premennej a zároveň platí $\langle v, (\exists z)\varrho\rangle \in S \equiv \langle v(x \longmapsto v(y)), (\exists z)\varrho\rangle \in S$, lebo iba ohodnotenie formálnych premenných majúcich vo formálnej formuli π voľné výskyty rozhoduje o platnosti formálnej formule $\langle v, \pi\rangle \in S$, ako je to zadefinované vo formuli (1) v dôkaze Vety 1.

- Teraz sústreďme našu pozornosť na formálnu formulu $(\exists y)\varrho$. Kvôli substituovateľnosti nesmie mať ϱ voľné výskyty formálnej premennej x. Z toho dôvodu je formálna formula $(\exists y)\varrho$ opäť totožná s formálnou formulou $[(\exists y)\varrho](x/y)$ a taktiež opäť platí $\langle v, (\exists y)\varrho\rangle \in S \equiv \langle v(x \longmapsto v(y)), (\exists y)\varrho\rangle \in S$.

- V poslednom prípade budeme musieť využiť indukčného predpokladu pre formálnu formulu ϱ a pre ohodnotenie $v(z \longmapsto z)$, kedy je formálna premenná z rôzna od y i x. Pre ľubovoľné x, y si preto predstavme, že ohodnotenie $[v(z \longmapsto z)](x \longmapsto x)$ je zhodné s ohodnotením $[v(x \longmapsto x)](z \longmapsto z)$. Takže platí:
  $\langle v, (\exists z)\varrho(x/y)\rangle \in S \equiv$
  $(\exists z)(\langle v(z \longmapsto z), \varrho(x/y)\rangle \in S) \equiv$
  $(\exists z)(\langle [v(z \longmapsto z)](x \longmapsto v(y)), \varrho\rangle \in S) \equiv$
  $(\exists z)(\langle [v(x \longmapsto v(y))](z \longmapsto z), \varrho\rangle \in S) \equiv$
  $\langle v(x \longmapsto v(y)), (\exists z)\varrho\rangle \in S$.

Na preukázanie tvrdení o formálnych prípadoch schémy špecifikácie použijeme schému špecifikácie z axiómov logického kalkulu. Predpokladali sme, že formálna premenná y je formálne substituovateľná do π za formálnu premennú x.

Z tohto práve dokázaného vzťahu dostávame $\langle v, (\forall x)\pi \to \pi(x/y)\rangle \in R \equiv [\langle v, (\forall x)\pi\rangle \in R \to \langle v, \pi(x/y)\rangle \in R] \equiv [(\forall x)(\langle v(x \longmapsto x), \pi\rangle \in R) \to \langle v(x \longmapsto v(y)), \pi\rangle \in R]$. Schému špecifikácie stačí skúmať len pre prípad nahrádzania premennej premennou, keďže nie je v jazyku teórie množín ako základný symbol žiadna funkcia ani konštanta.

Uvažujme, že formálna premenná x nie je voľná vo formálnej formuli π pri vyšetrovaní formálnych axiómov distribúcie. Potom platí $\langle v, (\forall x)(\pi \to \varrho) \to (\pi \to (\forall x)\varrho)\rangle \in R \equiv ((\forall x)[\langle v(x \longmapsto x), \pi\rangle \in R \to \langle v(x \longmapsto x), \varrho\rangle \in R] \to [\langle v, \pi\rangle \in R \to (\forall x)(\langle v(x \longmapsto x), \varrho\rangle \in R)])$. Už si len uvedomme, že na základe platnosti $\langle v(x \longmapsto x), \pi\rangle \in R \equiv \langle v, \pi\rangle \in R$, ktorej základom je predpoklad, že x nie je v π voľnou premennou a na základe využitia axiómu distribúcie z logického kalkulu, vyhovuje akékoľvek ohodnotenie druhej formuli.

Zjednodušenie axiómov rovnosti ponúka axióm extenzionality, takže umožňuje požadovať iba formulu $x = y \wedge x \in z) \to y \in z$. Stanovme preto φ buď ako hociktorý axióm ZF teórie množín okrem niektorého z axiómov nahradenia alebo ako uzáver spomenutej formule $x = y \wedge x \in z) \to y \in z$. Potom platí pre ľubovoľné ohodnotenie v podľa Vety 1: $(\Phi(R, X) \wedge \varphi \in X) \to (\varphi \equiv \langle v, \varphi\rangle \in R)$. Tvrdenie Vety 4 stačí dokázať už len pre formálne axiómy, ktoré sú v tvare schémy nahradenia, keďže formalizáciami axiómov ZF teórie sú všetky príslušné formálne axiómy formalizácie ZF teórie bez schémy nahradenia.

Na formalizácie prípadov schémy nahradenia sa pri skúmaní schémy nahradenia nemôžeme obmedziť, pretože musíme dokázať naše tvrdenia pre všetky formálne formule tvaru schémy nahradenia. Že formalizáciou niektorej metamatematickej formule je každá formálna formula, nám nič nezaručuje. Akokoľvek, pre každé ohodnotenie v a pre každé x nám z predpokladu $\langle v(x \longmapsto x), (\forall y, e, e')[(\pi \wedge \pi(e/e') \wedge y \in x) \to e = e']\rangle \in R$ a formule ekvivalencie (2) vyplýva, že v zmysle teórie množín je nasledujúca trieda funkciou: $F = \{\langle e, y\rangle; \langle v(x \longmapsto x, y \longmapsto y, e \longmapsto e), \pi \wedge y \in x\rangle \in R\}$. Pre myslené x je trieda $F''x$ množinou kvôli dôsledku axiómu nahradenia GB teórie množín, pričom platí formula $(\forall e)[e \in F''x \equiv (\exists y)(y \in x \wedge \langle e, y\rangle \in F)]$, z ktorej vyplýva, že vo formálnej formuli π formálna premenná z nie je voľná: $(\forall e)(v(x \longmapsto x, z \longmapsto F''x, e \longmapsto e)(e) \in v(x \longmapsto x, z \longmapsto F''x, e \longmapsto e)(z) \equiv (\exists y)[v(x \longmapsto x, y \longmapsto y, e \longmapsto e)(y) \in v(x \longmapsto x, y \longmapsto y, e \longmapsto e)(x) \wedge \langle v(x \longmapsto x, y \longmapsto y, e \longmapsto e), \pi\rangle \in R])$. Z uvedeného vyplýva

$$\langle v(x \longmapsto x), (\exists z)(\forall e)[e \in z \equiv (\exists y)(y \in x \wedge \pi)]\rangle \in R,$$

čím sme demonštrovali tvrdený vzťah $\langle v(x \longmapsto x), (\forall y, e, e')[(\pi \wedge \pi(e/e') \wedge y \in x) \to e = e']\rangle \in R \to \langle v(x \longmapsto x), (\exists z)(\forall e)[e \in z \equiv (\exists y)(y \in x \wedge \pi)]\rangle \in R$.

■

Dôkazy predchádzajúcich dvoch tvrdení nám posúžia v dôkaze Vety 5, kde budeme demonštrovať, že v našej štruktúre pri každom ohodnotení, ktorého definičný obor obsahuje formálne voľné premenné uvažovanej formálnej formule, je každá formálna formula formálne dokázateľná v ZF teórií, pravdivá.

Věta 5.5 *Pre každé ohodnotenie, ktoré je definované na všetkých formálnych voľných premenných formálnej formule π, platí v teórií GB vzťah $\langle v, \pi \rangle \in R$ ak $\Phi(R, X)$ a ak je π formálne dokázateľná vo formálnej ZF teórií formálnym dôkazom, ktorého všetky formálne formule sú prvkami triedy X.*

Důkaz. Stačí už len dokázať správnosť formálnych odvodzovacích pravidiel, pretože sme už v teórií GB dokázali tvrdenia pre všetky formálne axiómy ZF teórie a všetky formálne axiómy logického kalkulu. Za našich predpokladov indukcie podľa dĺžky formálneho dôkazu vo formálnej teórií ZF, demonštruujeme dôkaz tvrdenia vo Vete 5. Uvažujme teda, že máme vzťah $\langle v', \pi \rightarrow \varrho \rangle \in R$ pre každé ohodnotenie v', ktorého definičný obor obsahuje všetky formálne voľné premenné formálnej formule $\pi \rightarrow \varrho$ a zároveň uvažujme, že platí $\langle v'', \pi \rangle \in R$ pre každé ohodnotenie v'', ktorého definičný obor obsahuje všetky formálne voľné premenné formálnej formule π. Predpokladajme ohodnotenie v, ktorého definičný obor obsahuje všetky formálne voľné premenné formálnej formule ϱ. Ohodnotenie v rozšírme do ohodnotenia v', pričom v' je taktiež definované na všetkých formálnych voľných premenných formálnej formule π, takže dostávame vzťahy $\langle v', \pi \rightarrow \varrho \rangle \in R$ a zároveň $\langle v', \pi \rangle \in R$. Z uvedeného vyplýva $(\langle v', \pi \rightarrow \varrho \rangle \in R \wedge \langle v', \pi \rangle \in R) \rightarrow \langle v', \varrho \rangle \in R$, z čoho odvodíme platnosť $\langle v', \varrho \rangle \in R$. Zvážme, že hodnotenia v a v' sa na formálnych voľných premenných formule ϱ zhodujú, tak dostávame taktiež $\langle v, \varrho \rangle \in R$, čím dokazujeme, že formálne pravidlo modus ponens je pravidlom korektným.

Pre formálne pravidlo generalizácie uvážme, že máme vzťah $\langle v', \pi \rangle \in R$ pre každé také ohodnotenie v', ktorého definičný obor obsahuje všetky formálne voľné premenné formálnej formule π. Pre každé x a pre každé ohodnotenie v, ktorého definičný obor obsahuje všetky formálne voľné premenné formálnej formule $(\forall x)\pi$, platí ohodnotenie $v(x \longmapsto x)$. Definičný obor tohto ohodnotenia obsahuje všetky formálne voľné premenné formálnej formule π, takže z toho vyplýva vzťah $\langle v(x \longmapsto x), \pi \rangle \in R$, z ktorého získame $(\forall x)(\langle v(x \longmapsto x), \pi \rangle \in R)$, čiže $\langle v, (\forall x)\pi \rangle \in R$. ■

Definice 5.1 *V KM teórií definujme* $Sat = \{\langle v, \pi \rangle; (\exists R, X)(\Phi(R, X) \wedge \langle v, \pi \rangle \in R)\}$.

Keďže príslušná trieda je definovaná nenormálnou metamatematickou formulou, v ktorej sa nachádza kvantifikácia triednej premennej R (kvantifikáciou množinovej premennej by bolo možné nahradiť kvantifikáciu triednej premennej X, keďže množinou je každá časť množiny $Form$), nemusí mať zmysel uvedená definícia relácie splňovania v GB teórií.

Věta 5.6 *V KM teórií existuje formula* $\Phi(Sat, Form)$.

Důkaz. Ak platí $\pi \in X \wedge \Phi(R, X)$, potom je podľa Vety 1 $\langle v, \pi \rangle \in Sat \equiv \langle v, \pi \rangle \in R$. Nech najmenším prvkom množiny $Form$ je π také, že neexistuje X a R a to tak, že $\Phi(R, X) \wedge \pi \in X$. Tak je formálna formula π buď formálnou kvantifikáciou alebo formálnou konjunkciou, alebo formálnou negáciou svojej formálnej podformule/podformulí. Potom existuje S a Y ku každej formálnej podformuli ϱ formálnej formule π tak, že platí

$\Phi(S, Y) \wedge \varrho \in Y$. Vtedy ale existenciu R, X s vlastnosťou $\Phi(R, X) \wedge \pi \in X$ zaručuje Veta 2. Vzhľadom k nášmu predpokladu to ale vedie ku sporu. ∎

Věta 5.7 *Množinová formula $Con(ZF)$ je dokázateľná v KM teórií. Nie je ale dokázateľná v teórií ZF, za predpokladu bezospornosti teórie ZF.*

Důkaz. Neexistuje taká formálna formula π, ktorá by bola vo formálnej ZF teórií aj so svojou formálnou negáciou formálne dokázateľná. Ak by taká existovala, tak by podľa Viet 5 a 6 muselo byť $\langle v, \pi \rangle \in Sat \wedge \langle v, \neg\pi \rangle \in Sat$, pre každé ohodnotenie v zadefinované na všetkých formálnych voľných premenných formálnej formule π, a to by bolo v rozpore s platnosťou $\langle v, \neg\pi \rangle \in Sat \equiv \langle v, \pi \rangle \notin Sat$. Môžeme tvrdiť, že množinovou formulou je formula $Prf_{ZF}(d, \pi)$, ktorá popisuje, že d je formálnym dôkazom formálnej formule π vo formálnej teórií ZF. Formula $\neg(\exists d, \pi)Prf_{ZF}(d, \pi \wedge \neg\pi)$ je taktiež množinovou formulou, ktorá definuje, že súčasne neexistujú formálna formula π a d také, že d by bolo vo formálnej teórií ZF formálnym dôkazom $\pi \wedge \neg\pi$. Formula $\neg(\exists d, \pi)Prf_{ZF}(d, \pi \wedge \neg\pi)$ býva označovaná ako $Con(ZF)$ a v dôsledku druhej Gödelovej vety o neúplnosti nemôže byť dokázateľná v ZF teórií množín.

∎

Pri spracovaní kapitoly sme čerpali zo zdrojov [6], [2], [5], [9].

6 Finitnosť Gödel-Bernaysovej teórie množín

V štandardnej GB teórií množín je axióm zabezpečujúci existenciu triedy množín s určitou vlastnosťou Φ pridávaný pre každú formulu Φ jazyka teórie množín s triedami, v ktorých sú kvantifikované triedne premenné. Z toho môžeme zdanlivo vyvodiť záver, že schéma existencie tried vyžaduje nekonečne veľa axiómov. Ak ale nahradíme schému existencie tried axiómami:

$(\exists Z)(\forall e)[e \in Z \equiv (\exists x, y)(e = \langle x, y \rangle \wedge x \in y)]$,
$(\forall X, Y)(\exists Z)(\forall e)[e \in Z \equiv (e \in X \wedge e \notin Y)]$,
$(\forall X)(\exists Z)(\forall e)[e \in Z \equiv (\exists x)(\langle x, e \rangle \in X)]$,
$(\forall X, Y)(\exists Z)(\forall e)[e \in Z \equiv (\exists x, y)(e = \langle x, y \rangle \wedge e \in X \wedge y \in Y)]$,
$(\forall X)(\exists Z)(\forall e)[e \in Z \equiv (\exists x, y)(e = \langle x, y \rangle \wedge \langle y, x \rangle \in X)]$ a
$(\forall X)(\exists Z)(\forall e)[e \in Z \equiv (\exists x, y, z)(e = \langle x, y, z \rangle \wedge \langle y, z, x \rangle \in X)]$, pričom všetky uvedené axiómy sú špeciálne prípady schémy existencie tried (kde každý vychádza z nejakej konkrétnej normálnej formule) a takto upravenú GB teóriu doplníme o už spomenuté definície:

neusporiadanej dvojice ($Z = \{x, y\} \equiv (\forall e)[e \in Z \equiv (e = x \vee e = y)]$),
usporiadanej dvojice ($Z = \langle X, Y \rangle \equiv Z = \{\{X\}, \{X, Y\}\}$),
usporiadanej k-tice, kde $k > 2$ ($Z = \langle X_1, X_2, ..., X_k \rangle \equiv Z = \langle X_1 \langle X_2, ..., X_k \rangle \rangle$) a
usporiadanej k-tice, kde $k = 1$ ($Z = \langle X \rangle \equiv Z = X$), dostaneme z takto upravenej a doplnenej GB teórie tzv. **finitnú verziu GB** teórie množín (FGB).

Z uvedených axiómov nahradzujúcich špeciálne prípady schémy existencie tried získavame v poradí, v akom sú axiómy uvedené, obohatenie jazyka teórie množín o definíciu
konštanty náležania E: $Z = E \equiv (\forall e)[e \in z \equiv (\exists x, y)(e = \langle x, y \rangle \wedge x \in y)]$ a o definície funkcií:

rozdielu: $Z = X - Y \equiv (\forall e)[e \in Z \equiv (e \in X \wedge e \notin Y)]$,
definičného oboru: $Z = Dom(X) \equiv (\forall e)[e \in z \equiv (\exists y)(\langle y, e \rangle \in X)]$,
reštrikcie: $Z = X \upharpoonright Y \equiv (\forall e)[e \in Z \equiv (\exists x, y)(e = \langle x, y \rangle \wedge e \in X \wedge y \in Y)]$,
konverzie: $Z = X^{-1} \equiv (\forall e)[e \in Z \equiv (\exists x, y)(e = \langle x, y \rangle \wedge \langle y, x \rangle \in X)]$ a
trojnej konverzie: $Z = Con_3(X) \equiv (\forall e)[e \in Z \equiv (\exists x, y, z)(e = \langle x, y, z \rangle \wedge \langle y, z, x \rangle \in X)]$,
pričom takto obohatený jazyk teórie množín rozšírime ešte doplňujúcimi ekvivalenciami:
$Z = Rng(X) \equiv Z = Dom(X^{-1})$; $Z = V \equiv Z = Rng(E)$;
$Z = \varnothing \equiv Z = V - V$; $Z = X \cap Y \equiv Z = X - (X - Y)$;
$Z = X \times Y \equiv Z = (V \upharpoonright Y) \cap (V \upharpoonright X)^{-1}$; $Z = X^1 \equiv Z = X$ (pre ľubovoľnú triedu X) a
$Z = X^{k+1} \equiv Z = X \times X^k$ (pre ľubovoľné kladné prirodzené číslo k).

Z teórie FGB sme týmito rozšíreniami získali jej konzervatívne rozšírenie, ktoré budeme značiť FGB'. Na druhú stranu, faktom je, že teória GB konzervatívne obohatená definíciami neusporiadanej dvojice, usporiadanej dvojice, usporiadanej k-tice, kde $k > 2$ a usporiadanej k-tice, kde $k = 1$, je rozšírením FGB. Dôkaz nasledujúcej vety zase bude demonštrovať opak, teda, že teória FGB a FGB' sú rozšírením GB.

Věta 6.1 *V jazyku FGB′ teórie existuje term* $T(X_1, ..., X_n)$*, pre každú normálnu formulu* $\Phi(e, X_1, ..., X_n)$ *v jazyku teórie množín, taký, že platí* $FGB' \vdash (\forall e)(e \in T \equiv \Phi(e, X_1, ..., X_n))$*. Teda ak sú GB a FGB ekvivalentné, platí* $FGB \vdash (\exists Z)(\forall e)(e \in Z \equiv \Phi(e, X_1, ..., X_n))$*.*

Důkaz. Z vety o ekvivalencii (ktorá popisuje, že ak formula β vznikne z formule α nahradením niektorých jej výskytov podformúl $\gamma_1, ..., \gamma_k$ po rade formulami $\delta_1, ..., \delta_k$, tak potom platí $\gamma_1 \equiv \delta_1, ..., \gamma_k \equiv \delta_k \vdash \alpha \equiv \beta$) vyplýva, že ak demonštruujeme vetu pre formulu Φ, potom platí taktiež aj pre každú formulu Ψ, pre ktorú $FGB' \vdash \Phi \equiv \Psi$. Takže platí $\Phi \equiv \Psi \vdash (\forall e)(e \in T \equiv \Phi) \equiv (\forall e)(e \in T \equiv \Psi)$, čiže je potrebné dôkaz robiť len pre formule s určitými prídavnými vlastnosťami. Uvažujme takú normálnou formulu Φ, pre ktorú platí, že maximálne premenné $e, X_1, ..., X_n$ v nej majú voľné výskyty a súčasne voľné aj viazané výskyty v nej nemá žiadna premenná. Jednou z premenných musí byť $X_1, ..., X_n$, ak má triedna premenná výskyt vo formuli Φ, pretože všetky kvantifikované premenné musia byť množinové, keďže formula Φ je normálna. Treba ale upozorniť, že množinové premenné môžu zastupovať aj znaky $X_1, ..., X_n$, vtedy $X_1, ..., X_n \equiv x_1, ..., x_n$.

Premenné $X_1, ..., X_n$ budú medzi ostatnými premennými jedinečné, pretože budú reprezentovať parametre konštrukcie. Takže z toho vyplýva, že od nich bude závisieť výsledok konštrukcie, teda term T, ktorý má maximálne $X_1, ..., X_n$ ako svoje voľné premenné.

Formulou $(\exists z)(z = X_i \wedge z \in U)$ (v ktorej volíme za množinovú premennú z akúkoľvek premennú nenachádzajúcu sa vo formuli Φ) nahraďme v Φ jeden každý výskyt podformule v tvare $X_i \in U$ (U je ľubovoľná premenná). Formulu získanú týmto spôsobom označíme Θ. Formulou $(\forall z')(z' \in U \equiv z' \in W)$ (v ktorej volíme premennú z' tak, aby nemala výskyt v Θ) nahraďme v Θ jeden každý výskyt podformule v tvare $U = W$ (U, W sú ľubovoľné premenné, môžu byť aj množinové). Formulu získanú týmto spôsobom označíme Ψ. Zamenenie parametrov na ľavej strane pri symbole $\in$ vedie v uvedenom prvom nahradení k tomu, že sa už nevyskytuje triedna premenná na ľavej strane symbolu $\in$. V druhom nahradení ide o vynechanie symbolu $=$, preto sme museli zámenu uskutočniť rovnako pre parametre, ako aj pre ostatné premenné. Nie je už potrebné opakovať prvé nahradenie, keďže sme tým vo formuli Ψ nedostali žiadnu podformulu, v ktorej by bol parameter na ľavej strane symbolu $\in$. Formula $(\exists z)(z = X \wedge z \in U) \rightarrow X \in U$ je v FGB možné dokázať pomocou axiómu rovnosti z logického kalkulu v dôsledku formule $(Z = X \wedge Z \in U) \rightarrow X \in U$. Zavedením premenných pre množiny získame opačnú implikáciu, keďže platí $X \in U \rightarrow (\exists z)(z = X)$. Použitím vety o ekvivalencii a tranzitivity dokázateľnosti dostávame $FGB \vdash \Phi \equiv \Theta$. Aplikáciou axiómu extenzionality a znova vety o ekvivalencii dostaneme $FGB \vdash \Theta \equiv \Psi$ a $FGB \vdash \Phi \equiv \Psi$ získame tranzitivitou ekvivalencie.

Podarilo sa nám zdôvodniť predpoklad, že predstavovaná formula Φ má iba atomické formule typu $z \in x$ a $z \in X$, a to bez straty všeobecnosti. Veta o prenexnom tvare nám umožňuje predpokladať formulu Φ, ktorá je v tvare $(Q_k y_k)...(Q_1 y_1)\tilde{\Phi}$. Formula $\tilde{\Phi}$ neobsahuje kvantifikátor, čiže je otvorená a pre každé $1 \leq i \leq k$ v Q_i je jeden zo symbolov $\forall$ alebo $\exists$. Budeme uvažovať, že medzi premennými $y_1, ..., y_{k+1}, X_1, ..., X_n$ sú všetky voľné premenné formule $\tilde{\Phi}$. Pre ľubovoľnú otvorenú formulu Θ, ktorej všetky voľné premenné sú z premenných $y_1, ..., y_{k+1}, X_1, ..., X_n$, ktorá má atomické formule iba typu $z \in x$ a $z \in X$ a ktorá je podformulou formule Φ, zkonštruujeme term T_Θ indukciou podľa zložitosti formule Θ. Dodržíme pritom platnosť $FGB' \vdash (\forall y_1, ..., y_{k+1})(\langle y_1, ..., y_{k+1}\rangle \in T_\Theta \equiv \Theta)$. V terme T_Θ sa môžu vyskytovať premenné $X_1, ..., X_n$, pretože sú považované za parametre konštrukcie. Term T_Θ konštruujeme v teórií FGB′ s prístupom ku všetkým jej konštantám a funkciám:

(1) Uvážme formulu Θ v tvare $y_i \in X_j$.
Pre i, j platí: $1 \leq i \leq k+1$ a $1 \leq j \leq n$. Potom existujú tieto prípady:

- $k = 0$ - ak máme iba premennú y_1 namiesto systému premenných $y_1, ..., y_{k+1}$, potom $T_\Theta = X_j$
- $k > 0$ a $i = 1$ - potom $T_\Theta = X_j \times V^k$
- $k > 0$ a $1 < i \leq k$ - potom $T_\Theta = V \times (...(V \times (X_j \times V^{k-i+1}))...)$ (násobenie $V \times ...$ uskutočňujeme $(i-1)$-krát a počet zátvoriek každého typu je $i-1$)
- $k > 0$ a $i = k+1$ - potom $T_\Theta = V \times (...(V \times X_j)...)$ (násobenie $V \times ...$ uskutočňujeme k)-krát a počet zátvoriek každého typu je $k-1$)

V každej z uvedených možností platí vzťah $FGB' \vdash (\forall y_1, ..., y_{k+1})(\langle y_1, ..., y_{k+1}\rangle \in T_\Theta \equiv y_i \in X_j)$.

(2) Uvážme formulu Θ v tvare $y_i \in y_j$.
Zaveďme pomocné termy S_1, S_2, S_3 tak, že konštrukcia termu S_2 podlieha možnej existencii premenných *vzadu* a navyše konštrukcia termu S_3 počíta s možnou existenciou premenných *medzi* premennými y_i a y_j a možnú existenciu premenných *vpredu* rešpektuje finálna konštrukcia termu T_Θ. Potom:

- definujme $S_1 = E$ za predpokladu $i < j$; $S_1 = E^{-1}$ za predpokladu $j < i$ a $S_1 = \varnothing$ za predpokladu $i = j$. Potom platí $FGB' \vdash \langle y_{min(i,j)}, y_{max(i,j)}\rangle \in S_1 \equiv y_i \in y_j$.
- definujme $S_2 = S_1$ za predpokladu $max(i,j) = k+1$ a definujme $S_2 = Con_3(Con_3$ $(V^{k-max(i,j)+1} \times S_1))$, za predpokladu $max(i,j) \leq k$. Keďže $FGB' \vdash [\langle x, y, z\rangle \in Con_3(Con_3(X)) \equiv \langle y, z, x\rangle \in Con_3(X)] \wedge [\langle y, z, x\rangle \in Con_3(X) \equiv \langle z, x, y\rangle \in X]$, tak potom získame $\langle y_{min(i,j)}, y_{max(i,j)}, y_{max(i,j)+1}, ..., y_{k+1}\rangle \in S_2 \equiv y_i \in y_j$. Ak nastane $max(i,j) = k+1$, tak sa $y_{max(i,j)+1}, ..., y_{k+1}$ v zápise vynechá a ak nastane $i = j$, tak sa $y_{max(i,j)}$ vynechá a zostane iba s ňou identická premenná $y_{min(i,j)}$.
- definujeme $S_3 = S_2$ za predpokladu $max(i,j) = min(i,j) + 1$ a definujeme $S_3 = Con_3(V \times ... \times Con_3(V \times (S_2)^{-1})...)$ za predpokladu $max(i,j) - min(i,j) > 1$. Operáciu $Con_3(V \times (...)^{-1})$ vykonávame $(max(i,j) - min(i,j) - 1)$-krát. Keďže $FGB' \vdash [\langle x, y, z\rangle \in Con_3(V \times X^{-1}) \equiv \langle y, z, x\rangle \in V \times X^{-1}] \wedge [\langle y, z, x\rangle \in V \times X^{-1} \equiv \langle z, x\rangle \in X^{-1}] \wedge [\langle z, x\rangle \in X^{-1} \equiv \langle x, z\rangle \in X]$, tak získame vzťah $FGB' \vdash \langle y_{min(i,j)}, y_{min(i,j)+1}, ..., y_{k+1}\rangle \in S_3 \equiv y_i \in y_j$

- definujeme $T_\Theta = S_3$ za predpokladu $min(i,j) = 1$ a definujeme $T_\Theta = V \times (... \times (V \times S_3)...)$ za predpokladu $min(i,j) > 1$. Operáciu $V \times (...)$ vykonávame $(min(i,j)-1)$-krát. Dostávame tak $FGB' \vdash \langle y_1, ..., y_{k+1} \rangle \in T_\Theta \equiv y_i \in y_j$.

(3) Uvážme formulu Θ v tvare $\Gamma \wedge \Delta$.
Definujeme $T_\Theta = T_\Gamma \cap T_\Delta$ pri indukčnom predpoklade už zadefinovaných termov T_Γ a T_Δ.
(4) Uvážme formulu Θ v tvare $\neg\Gamma$.
Definujeme $T_\Theta = V^{k+1} - T_\Gamma$ pri predpoklade už zadefinovaného termu T_Γ.

Teraz sa upriamime na zkonštruovanie termov T_Θ pre formule, ktoré dostaneme iterovanou množinovou kvantifikáciou. Takéto termy získame z vyššie definovaných formulí. Pre ľubovoľnú formulu Φ existuje formula Ψ taká, že pre ňu platí $FGB \vdash \Phi \equiv \Psi$ a existuje pre ňu definícia T_Ψ. Umožňuje nám to aplikácia vety o prenexnom tvare. Konštrukciu hľadaných termov začneme krokom, že indukciou stanovíme $T_{(\exists y)\Theta} = Dom(T_\Theta)$. Kombináciou bodu (4) a tejto definície prevedieme univerzálnu kvantifikáciu a definujeme $T_{(\forall z)\Theta} = V^m - Dom(T \neg \Theta)$, pričom m je počet premenných v systéme $y_1, ..., y_{k+1}$, ktoré vo formuli $(\forall z)\Theta$ nie sú kvantifikované. Keďže Φ je v tvare $(Q_k y_k)...(Q_1 y_1)\tilde{\Phi}$, tak idúc po kvantifikátoroch odzadu indukciou podľa $1 \leq i \leq k$ preukazujeme $(\forall X_1, ..., X_n)(\forall y_{i+1}, ..., y_{k+1})(\langle y_{i+1}, ..., y_{k+1} \rangle \in T_{(Q_i y_i)...(Q_1 y_1)\tilde{\Phi}} \equiv (Q_i y_i)...(Q_1 y_1)\tilde{\Phi})$. Takže platí $(\forall X_1, ..., X_n)(\forall y_{k+1})(y_{k+1} \in T_\Phi \equiv \Phi)$. Dokázali sme teda existenciu triedy s požadovanou vlastnosťou. ∎

Kapitolu sme spracovali pomocou zdrojov [2], [10].

7 Axióm výberu v teórií množín a hypotéza kontinua

Existencia množiny reálnych čísel, ktorá nemá rovnakú mohutnosť, ako množina všetkých reálnych čísiel a nie je ani najviac spočítateľná (spočítateľnou množinou je taká množina, ktorú je možné vzájomne jednoznačne zobraziť na množinu všetkých prirodzených čísel), patrí medzi základné otázky teórie množín. Hilbert (1862-1943) zaradil tento problém do zoznamu najväčších matematických problémov svojej doby. Tento problém je pomenovaný ako **hypotéza kontinua**, označuje sa CH a zapisuje sa $2^{\aleph_0} = \aleph_1$. Tento zápis formuluje, že potencia $P(\omega)$ má mohutnosť rovnú najmenšiemu nespočítateľnému kardinálnemu číslu. *Zobecnená hypotéza kontinua (GCH)* sa zapisuje $(\forall \alpha \in On)(2^{\aleph_\alpha} = \aleph_{\alpha+1})$, ($On$ ožnačuje triedu ordinálnych čísel) a popisuje, že je mohutnosť množiny všetkých podmnožín pre každé kardinálne číslo k akejkoľvek mohutnosti k najmenšie možné kardinálne číslo, teda také kardinálne číslo, ktoré nasleduje bezprostredne za kardinálnym číslom k v usporiadaní kardinálnych čísel. K ďalšiemu problému teórií množín radíme otázku, či je v nej **Axióm výberu** (*AC*) dokázateľný. Axióm výberu je formula

$$(\forall x)(\exists f)[Fnc(f) \wedge Dom(f) = x \wedge (\forall y \in x)(y \neq \varnothing \rightarrow f(y) \in y)]$$

pričom označenie $Fnc(f)$ symbolizuje konzervatívny zápis unárneho predikátu „byť funkciou“ v jazyku teórie množín a vo všeobecnosti je definovaný zápisom $Fnc(x) \equiv (Rel(x) \wedge (\forall z, e_1, e_2)[(\langle e_1, z\rangle \in x \wedge \langle e_2, z\rangle \in x) \rightarrow e_1 = e_2])$, kde $Rel(x)$ symbolizuje unárny predikát „byť reláciou“, reprezentovaný zápisom $Rel(x) \equiv (\forall e)[e \in x \rightarrow (\exists x, y)(e = \langle x, y\rangle)]$

a zápis $Dom(f)$ definuje funkciu definičného oboru, všeobecný zápis je $z = Dom(x) \equiv (\forall e)[e \in z \equiv (\exists y)(\langle y, e\rangle \in x)]$, kde z reprezentuje množinovú premennú.

Formula, ktorou je axióm výberu zapísaný, popisuje, že na každom neprázdnom súbore neprázdnych množín existuje tzv. *selektor*, ktorý je možné definovať ako funkciu, ktorá vyberá práve jeden prvok z každej množiny tohto súboru. Od ostatných axiómov sa tento axióm líši tým, že je nekonštruktívny. Ak iné axiómy určujú existenciu nejakej množiny, nejakou formulou definujú jej vlastnosti, u tohto axiómu to tak nie je. Ale ak je nejaká množina konečná, je možné dokázať existenciu selektoru. Vzhľadom k tomu, axióm výberu sa v matematike štandardne uplatňuje. S axiómami ZF teórie nie je v rozpore, neodporuje intuícií a bez jeho existencie by nebolo možné dokázať niektoré podstatné tvrdenia napríklad v algebre, topológií alebo vo funkcionálnej analýze. Axióm výberu je ekvivalentný s *princípom dobrého usporiadania*, ktorý sa dá popísať tak, že dobré usporiadanie existuje na každej množine.

Matematici neboli schopný vyriešiť dokázateľnosť AC a CH až do objavu Gödela (1906-1978) v roku 1940, ktorý ukázal, že oba tieto problémy možno bezosporne pridať k ZF teórii. Objav bol založený na dôkaze, že pri predpoklade bezospornosti ZF teórie v nej nemožno preukázať ani negáciu AC ani negáciu CH. Toto bol ním zatiaľ iba polovične zostrojený dôkaz, ktorý zúplnil až v šesťdesiatych rokoch minulého storočia tým, že zostrojil triedu **L** *konštruovateľných* množín založených na princípe, že postupne sú takéto množiny konštruované na základe už zostrojených množín.

ZF teória s prijatým AC a CH je tak len obyčajné obmedzenie množín na systém zkonštruovateľných množín so zachovanou platnosťou predikátov rovnosti aj náležania vo všeobecnej ZF teórií.

Vo všeobecnosti štruktúra $\langle a, E \cap a^2 \rangle$ zodpovedá formálnemu modelu nejakej formálnej teórie jazyka teórie množín, kde druh možných premenných x definuje formula $x \in a$, pričom a je univerzom tohto modelu. Uvedená formula je absolútna v tomto modeli práve keď je absolútna v takto popísanej interpretácií. Absolútnosťou formule teórie množín v uvedenej štruktúre pre jazyk teórie množín s univerzom a, ktoré je množinou, sa myslí platnosť definovaná zápisom $(\forall x_1, ..., x_n \in a)(\varphi(x_1, ..., x_n) \equiv \langle a, E \cap a^2 \rangle \models \varphi[x_1, ..., x_n])$, kde φ reprezentuje axióm formálnej teórie.

Princíp konštruovateľných množín vychádza z nasledujúceho popisu:

Definice 7.1 *Pre každú množinu x nech $Df(x)$ označuje systém všetkých podmnožín z množiny z, ktoré sú definovateľné v štruktúre $\langle x, E \cap x^2 \rangle$ (symbol E tu reprezentuje konštantu náležania definovanú zápisom $z = E \equiv (\forall e)[e \in z \equiv (\exists x, y)(e = \langle x, y \rangle \wedge x \in y)]$) s parametrami z tejto štruktúry, tzn. pre ktoré existuje formálna formula $\pi(y, x_1, ..., x_n)$ jazyka teórie množín a množiny $x_1, ..., x_n \in x$ tak, že:*

$$z = \{y \in x; \langle x, E \cap x^2 \rangle \models \pi[y, x_1, ..., x_n]\}$$

Pre každé $\alpha \in On$ zostrojme transfinitnou rekurziou množiny L_α a navyše zaveďme triedu L definujúcu:

- $L_0 = \varnothing$
- $L_{\alpha+1} = Df(L_\alpha)$ *pre ľubovoľné ordinálne číslo* α
- $L_\lambda = \bigcup\{L_\alpha; \alpha \in \lambda\}$ *pre ľubovoľné limitné ordinálne číslo* λ
- $L = \bigcup\{L_\alpha; \alpha \in On\}$

Symbol $\bigcup$ značí unárnu funkciu zjednotenia triedy a je definovaný predpisom $z = \bigcup x \equiv (\forall e)[e \in z \equiv (\exists y)(e \in y \wedge y \in x)]$

Věta 7.1 *V ZF teórií množín je možné dokázať formule:*

- ***(1)*** $(y \in z \wedge z \in L_\alpha) \rightarrow y \in L_\alpha$ *(L_α je tranzitívna)*
- ***(2)*** $\alpha \in \beta \rightarrow L_\alpha \in L_\beta$
- ***(3)*** $\alpha \in L_{\alpha+1} - L_\alpha$

Důkaz. Dôkaz robíme v ZF teórií. Tvrdenie (1) dokazujeme pomocou indukcie podľa ordinálnych čísel doplnenou tvrdením (1a) $\alpha \in \beta \rightarrow L_\alpha \subseteq L_\beta$.

Nech je ε najmenšie zo všetkých ordinálnych čísel α, pre ktoré neplatí implikácia $(\forall y, z)[(y \in z \wedge z \in L_\alpha) \rightarrow y \in L_\alpha]$ alebo existuje také $\beta \ni \alpha$, že neplatí (1a). $L_0 = \varnothing$ je tranzitívne a $\varnothing \subseteq z$ pre ľubovoľné z, preto nemôže byť $\xi = 0$. Najskôr predpokladajme, že neplatí $(\forall y, z)[(y \in z \wedge z \in L_\xi) \rightarrow y \in L_\xi]$. Potom priamo z definície nemôže byť ξ limitné. Teda $\xi = \gamma + 1$ pre nejaké $\gamma \in On$. $z \subseteq L_\gamma$ plynie z definície množiny L_ξ a zo vzťahu $z \in L_\xi$, takže platí, že $y \in L_\gamma$. $y \in L_\xi$ nám zaručuje tvrdenie (1a) aplikované na $\gamma \in \xi$, takže dochádzame ku sporu.

Z toho nám vyplýva, že $L_\xi \subseteq L_\beta$ pre nejaké $\beta \ni \xi$ neplatí povinne pre číslo ξ. Pre najmenšie $\beta \ni \xi$, pre ktoré neplatí skúmaná inklúzia, zvoľme ζ. Takže musí existovať $\delta \ni \xi$ taká, že $\zeta = \delta + 1$. V tomto dôsledku je $L_\xi \subseteq L_\delta$. Ak si predstavíme formulu $y \in z$, dostaneme pre ňu a pre akékoľvek $z \in L_\xi$

$$z = \{y \in L_\delta; \langle L_\delta, E \cap L_\delta^2 \rangle \models y \in z[y, z]\}$$

pretože $z \subseteq L_\delta$ je z dokázanej tranzitivity množiny L_ξ. Takže nám z toho vyplýva inklúzia $L_\xi \subseteq L_{\delta+1}$, ciže opäť dochádzame ku sporu.

Ak dokážeme vzťah $L_\alpha \in L_{\alpha+1}$ a použijeme tvrdenie (1a), dokážeme tvrdenie (2). Ak zvážime zadefinovanie množiny $L_{\alpha+1}$ a uvedomíme si rovnosť $L_\alpha = \{y \in L_\alpha; \langle L_\alpha, E \cap L_\alpha^2 \rangle \models y = y[y]\}$, dokážeme skúmaný vzťah náležania.

Dôkaz tvrdenia (3) začneme najskôr dôkazom vzťahu $\alpha \notin L_\alpha$. Definujeme ξ ako najmenšie α, pričom $\alpha \in L_\alpha$, potom nemôže byť limitné ordinálne číslo ξ, lebo by pre nejaké $\beta \in \xi$ muselo byť $\xi \in L_\beta$. Z tranzitivity množiny L_β by vyplývalo $\beta \in L_\beta$, čiže spor. Pri vhodnom zvolení $\gamma \in On$ je $\xi = \gamma + 1$, potom ale podľa zadefinovania množiny $L_{\gamma+1}$ platí $\xi \subseteq L_\gamma$, takže vyplýva $\gamma \in L_\gamma$ a zase prichádzame ku sporu.

Pomocou sporu dokážeme platnosť vzťahu $\alpha \in L_{\alpha+1}$. Definujeme si ζ ako najmenšie ordinálne číslo α, pričom platí $\neg\alpha \in L_{\alpha+1}$. Ak je ζ limitné, platí, že $\zeta \subseteq \bigcup\{L_\beta; \beta \in \zeta\} = L_\zeta$. Ak ζ limitné nie je, vyplýva rovnaká inklúzia z tranzitivity množiny L_ζ. Z inklúzie $On \cap L_\zeta \subseteq \zeta$, ktorú získame z prvej časti dôkazu a z tranzitivity množiny L_ζ vyplýva $\zeta = On \cap L_\zeta$.

V teórií ZF je formula $Ord(y)$, ktorá definuje ordinálne čísla, obmedzená. Preto $ZF \vdash (\forall x)(\forall y \in x)[Tran(x) \rightarrow (Ord(y) \equiv \langle x, E \cap x^2 \rangle \models Ord(y)[y])]$ (kde symbol $Tran(x)$ reprezentuje tranzitívnu množinu, tj. takú, pre ktorú platí $(\forall x, y)[(x \in y \wedge y \in x) \rightarrow x \in x]$), preto platí $ZF \vdash \zeta = L_\zeta \cap On = \{y \in L_\zeta; \langle L_\zeta, E \cap L_\zeta^2 \rangle \models Ord(y)[y]\} \in L_{\zeta+1}$.

■

Budeme uvažovať interpretáciu jazyka ZF teórie množín označenú ako ℓ, ktorá je tvorená formulami $x \in L$, $x \in y$ a $x = y$. Práve prvky triedy L budú objektami zostrojovanej interpretácie, v ktorej zadefinovaním formulí $x = y$ a $x \in y$ zaistíme absolútnosť predikátov rovnosti a náležania. Takže v teórií $ZF^{(\ell)}$ uvážme interpretáciu jazyka teórie množín, pričom do tohto jazyka doplníme predikáty $\in^\ell$, $=^\ell$, premenné nového druhu x^ℓ

a axiómy teórie $ZF^{(\ell)}$ doplnené o:

$(\exists x^\ell)(x = x^\ell) \equiv x \in L$
$x \in^\ell y \equiv x \in y$
$x =^\ell y \equiv x = y$

Věta 7.2 *Interpretácia ℓ ZF teórie množín je definovaná formulami $x \in L$, $x \in y$ a $x = y$, pričom $V = L$.*

Označenie $V = L$ zastupuje formulu $(\forall x)(\exists \alpha)(x \in L_\alpha)$, ktorá sa nazýva **Axióm konštruovateľnosti**. Symbol V reprezentuje konštantu pre univerzálnu triedu Z definovanú $Z = V \equiv (\forall e)(e \in Z \equiv e = e)$

Důkaz. V interpretácií ℓ teórie ZF^ℓ postupne overíme platnosť jednotlivých axiómov, ktoré sa zaoberajú dokázateľnosťou uvedených formulí v samotnej teórií ZF.

- *Axióm extenzionality* je uzáver obmedzenej formule $(\forall e)(e \in x \equiv e \in y)$. Vzhľadom k ℓ je každá obmedzená formula absolútna, takže aj skúmaná formula je absolútna. Taktiež pre každú formulu ϑ platí $(\forall x)\vartheta \rightarrow (\forall x \in L)\vartheta$.

- *Axióm zjednotenia* - pracujeme v teórií ZF, aby sme mohli najskôr preukázať, že $ZF \vdash x \in L \rightarrow \bigcup x \in L$. V dôsledku tranzitivity množiny L_α je $\bigcup x \subseteq L_\alpha$, ak $x \in L_\alpha$. Formula $z = \bigcup x \equiv (\forall e \in z)(\exists y \in x)(e \in y) \wedge (\forall y \in x)(\forall e \in y)(e \in z)$ definujúca $\bigcup x$ je obmedzená, takže je v štruktúrnom zápise $\langle L_\alpha, E \cap L_\alpha^2 \rangle$ absolútna. Platí preto:
$\bigcup x = \{e; (\exists y \in x)(e \in y)\} = \{e \in L_\alpha; \langle L_\alpha, E \cap L_\alpha^2 \rangle \models (\exists y \in x)(e \in y)[x, e]\} \in L_{\alpha+1}$
V súvislosti s uvažovanou interpretáciou je formula definujúca $\bigcup x$ absolútna, takže axióm zjednotenia platí v zmysle interpretácie ℓ.

- *Axióm potencie* - pre ľubovoľné $x \in L$ v ZF ukážeme, že $P(x) \cap L \in L$. Ak formulu dvoch premenných α, y, pričom $\alpha \in On \wedge y \in L_\alpha \wedge (\forall \beta \in On)(y \in L_\beta \rightarrow \alpha \in \beta)$ označuje ψ, možno na ňu schému nahradenia aplikovať a potom je možné dokázať existenciu takého ξ, že platí
$(\forall y \in P(x))(y \in L \rightarrow y \in L_\xi)$, prípadne $P(x) \cap L \subseteq L_\xi$.

  Potom ale $P(x) \cap L = \{y \in L_\xi; \langle L_\xi, E \cap L_\xi^2 \rangle \models y \subseteq x[x, y]\} \in L_{\xi+1}$. Formula $y \subseteq x$ je obmedzená a teda vzhľadom k interpretácií ℓ absolútna. Z toho plynie, že množina $P(x) \cap L$ je v zmysle interpretácie potenciou množiny x. V skúmanej teórií existuje x také, že $P(x) \neq P(x) \cap L$, v zmysle interpretácie ℓ nie je formula definujúca funkciu potencie v teórií ZF absolútna, $V \neq L$.

- *Axióm nahradenia* - uvažujeme ľubovoľnú formulu φ s dvomi voľnými premennými e a y na preukázanie schémy nahradenia. Budeme ju označovať φ^ℓ, pretože ju uvažujeme v zmysle interpretácie ℓ a jej premenné budú označené e^ℓ a y^ℓ. Zafixujeme

množinu $x \in L$ a aj ďalšie parametre formule φ^{ℓ} fixujeme ako prvky L. Potrebujeme v teórií $ZF^{(\ell)}$ s definovanými fixáciami z predpokladu
$(\forall y, e_1, e_2 \in L)([\varphi^{\ell}(e^{\ell}/e_1, y^{\ell}/y) \wedge \varphi^{\ell}(e^{\ell}/e_2, y^{\ell}/y) \wedge y \in x] \rightarrow e_1 = e_2)$ dokázať formulu

$$(\exists z \in L)(\forall e \in L)(e \in z \equiv (\exists y \in L)[y \in x \wedge \varphi^{\ell}(e^{\ell}/e, y^{\ell}/y)])$$

pre ktorú platí, že je ekvivalentná formuli $(\exists z \in L)(\forall e \in L)(e \in z \equiv (\exists y)[y \in x \wedge \varphi^{\ell}(e^{\ell}/e, y^{\ell}/y)])$ v dôsledku tranzitivity triedy L. Pre určené $x \in L$ definujeme:
$Z = \alpha \in On; (\exists y)(y \in x \wedge (\exists e)[\varphi^{\ell}(e^{\ell}/e, y^{\ell}/y) \wedge e \in L_{\alpha} \wedge (\forall \beta \in On)(e \in L_{\beta} \rightarrow \alpha \in \beta)])$. Formula $y \in x \wedge \alpha \in On \wedge (\exists e)[\varphi^{\ell}(e^{\ell}/e, y^{\ell}/y) \wedge e \in L_{\alpha} \wedge (\forall \beta \in On)(e \in L_{\beta} \rightarrow \alpha \in \beta)]$ predstavuje za definovaných predpokladov funkciu, čiže v dôsledku schémy nahradenia je trieda Z množinou. Z toho vyplýva, že musí existovať taká $\xi \in On$, že prvkami L_{ξ} sú všetky parametre a preto
$x \in L_{\xi} \wedge (\forall y \in x)[(\exists e \in L)\varphi^{\ell}(e^{\ell}/e, y^{\ell}/y) \rightarrow (\exists e \in L_{\xi})\varphi^{\ell}(e^{\ell}/e, y^{\ell}/y)]$.

Ďalej nájdeme λ tak, že $\xi \in \lambda \wedge \lambda \in On$ a pre ktorú platí $(\forall e, y \in L_{\lambda})(\varphi^{\ell}(e^{\ell}/e, y^{\ell}/y) \equiv \langle L_{\lambda}, E \cap L_{\lambda}\rangle \models \varphi[e, y])$. Uzatváraním na potrebné operácie vytvoríme konštrukciu, pre ktorú je dôležité že do triedy L sú obmedzené všetky kvantifikácie vo formuli φ^{ℓ}. Potom $e \in L; (\exists y)(y \in x \wedge \varphi^{\ell}(e^{\ell}/e, y^{\ell}/y)) = e \in L_{\lambda}; (\exists y)(y \in x \wedge \varphi^{\ell}(e^{\ell}/e, y^{\ell}/y)) = e \in L_{\lambda}; \langle L_{\lambda}, E \cap L_{\lambda}^2\rangle \models (\exists y)(y \in x \wedge \varphi)[x, e] \in L_{\lambda+1}$

- *Axióm nekonečna* - platí, že $\omega \in L$, pričom ω označuje konštantu reprezentujúcu množinu všetkých prirodzených čísel, pričom je v ZF teórií táto množina prvkom On. Axióm nekonečna je dôsledkom absolútnosti formule $(\exists z)[z \in x \wedge (\forall e)(e \notin z)] \wedge (\forall y)(y \in x \rightarrow (\exists z)[z \in x \wedge (\forall e)(e \in z \equiv (e \in y \vee e = y))])$, ktorá označuje formulu obmedzenú v teórií s jazykom teórie množín a bez mimologických axiómov.
- *Axióm fundovanosti* má tvar $(\forall x)\varphi$, pričom φ reprezentuje absolútnu formulu $(\exists y)(y \in x) \rightarrow (\exists y)[y \in x \wedge (\forall e)\neg(e \in y \wedge e \in x)]$. Z toho vyplýva, že je tento axióm ekvivalentný v ZF teórií formuli $(\forall x \in L)\varphi$ v zmysle interpretácie, takže je triviálnym dôsledkom formule $(\forall x)\varphi$.

V zmysle interpretácie ℓ dokážeme platnosť $V = L$. Taktiež, že aj pre každé $\alpha \in On$ je $L_{\alpha} = (L_{\alpha})^{\ell}$. K tomu potrebujeme overiť absolútnosť niektorých pojmov. Pripomenieme, že pojem „byť ordinálnym číslom“ je absolútny a platí $On \subseteq L$ a taktiež platí $\omega \subseteq L$, čiže ukázanie, že absolútny je aj pojem „byť prirodzeným číslom“ je možné tak, že nenulové prirodzené čísla sú práve tie ordinálnymi číslami α, také, že

$$\alpha \in \omega \equiv \alpha \in On \wedge (\forall x \in \alpha)(\exists y \in x)(x = y \cup \{y\})$$

čiže ktoré majú predchodcu a ktorých každý prvok má predchodcu. Pritom formula $z = \bigcup x$ definujúca zjednotenie $((\forall e \in z)(\exists y \in x)(e \in y) \wedge (\forall y \in x)(\forall e \in y)(e \in z))$ a formula $e \in \{x, y\}$ popisujúca neusporiadanú dvojicu $(e = x \vee e = y)$ sú tiež absolútne. Absolútnym nie je len pojem „byť prirodzeným číslom“, „byť funkciou“, zjednotenie, definičný obor atď, ale absolútnou je celá aritmetika. Aby sme to mohli dokázať, musíme dokázať tiež absolútnosť definície sčítania a násobenia prirodzených čísel. Dosiahneme to tak, že si ako prvé predstavíme, že pre každú konečnú množinu platí $x \subseteq L \to x \in L$. Takže tento vzťah platí ak $x = \{x_1, ..., x_n\} \subseteq L_\alpha$, kde $n \in \omega$, potom $x = \{e \in L_\alpha; \langle L_\alpha, E \cap L_\alpha^2\rangle \models (e = x_1 \vee ... \vee e = x_n)[x_1 \longmapsto x_1, ..., x_n \longmapsto x_n, e \longmapsto e]\}$, kde $x_1 \longmapsto x_1$ popisuje ohodnotenie, teda priradenie indivituí k voľným premenným formule.

Prirodzeným číslom l, pre ktoré existuje f, pre ktoré platí:

$Dom(f) = ((\{0\} \times n) \cup (\{1\} \times m)) \wedge Rng(f) = l \wedge Fnc(f) \wedge Fnc(f^{-1})$

je definovaný súčet prirodzených čísel n a m (pričom symbol Rng zastupuje funkciu oboru hodnôt definovanú $z = Rng(x) \equiv (\forall e)[e \in z \equiv (\exists y)(\langle e, y\rangle \in x)]$ a f^{-1} vyjadruje funkciu konverzie). Potom z uvedeného zápisu vyplýva, že $f \subseteq L$ je konečná, takže $f \in L$. Navyše táto funkcia zabezpečí $(n + m = l)^\ell$.

Absolútnosť definície násobenia overíme podobne. Súčin prirodzených čísel n, m je určený ako číslo l, pre ktoré f existuje tak, že:

$Dom(f) = n \times m \wedge Rng(f) = l \wedge Fnc(f) \wedge Fnc(f^{-1})$

Formulami je možné považovať niektoré prirodzené čísla, keďže je možné aritmetizovať syntax logiky. Takže musí byť absolútny aj pojem „byť formálnou formulou jazyka jazyka teórie množín“. Nebudeme tvrdiť, že každá štruktúra množín v jazyku teórie množín v tvare $\langle a, r\rangle$ musí byť prvkom L. Ale ak platí, že konštruovateľná je, potom je vlastnosť $\langle a, r\rangle \models \pi[x_1, ..., x_n]$ absolútna, keďže je iba jediná kvantifikácia v indukčnom kroku definície formálneho splňovania vo formálnej štruktúre. Táto kvantifikácia je v popise formálneho splňovania pre formálnu formulu, ktorá vznikla pri definovaní splňovania $\langle a, r\rangle \models [(\exists x)\pi][x_1 \longmapsto x_1, ..., x_n \longmapsto x_n]$, teda formálnou kvantifikáciou.

Je nutné sa zaoberať formulou $(\exists x \in a)(\langle a, r\rangle \models \pi[x \longmapsto x, x_1 \longmapsto x_1, ..., x_n \longmapsto x_n])$ v skúmanom indukčnom kroku, ale táto formula je absolútna, pretože má obmedzenú v nej potrebnú kvantifikáciu. Absolútnosť definície funkcie Df je možné dokázať na základe faktu, že prvkom L je aj každé ohodnotenie voľných formálnych premenných formálnej formule π prvkami triedy L.

Budeme predpokladať, že ξ je najmenšie α také, že $L_\alpha \neq (L_\alpha)^\ell$. Potom nemôže byť $\xi = 0$, keďže $L_0 = \varnothing = (L_0)^\ell$. Nemôže byť ani limitné, pretože potom by platilo:

$L_\xi = \bigcup\{L_\beta; \beta \in \xi\} = \bigcup\{(L_\beta)^\ell; \beta \in \xi\} = (L_\xi)^\ell$

vzhľadom na absolútnosť formule, ktorá definuje zjednotenie. ξ nemôže mať ani tvar $\gamma + 1$, pretože by potom platilo $L_{\gamma+1} = Df(L_\gamma) = Df((L_\gamma)^\ell) = [Df(L_\gamma)]^\ell = (L_{\gamma+1})^\ell$, kvôli absolútnosti definície funkcie Df.

To, že pre každé $\alpha \in On$ je $L_\alpha = (L_\alpha)^\ell$, zaručuje tento spor. Z toho vyplýva, že $(\exists \alpha \in On)(x \in L_\alpha)$ je ekvivalentné formuli $(\exists \alpha \in On^\ell)(x \in L_\alpha^\ell)$ a preto $(\forall x \in L)(\exists \alpha \in On)(x \in L_\alpha)$ je ekvivalentné $[(\forall x)(\exists \alpha \in On)(x \in L_\alpha)]^\ell$.

■

Podarilo sa nám dokázať absolútnosť viacerých pojmov, ale nie je pravda, že absolútne je všetko. Absolútna nemusí byť napríklad vlastnosť „byť kardinálnym číslom“. Ak neexistuje navzájom jednoznačná funkcia zobrazujúca α na $\beta \in \alpha$, je takáto α kardinálne číslo, ale ak existuje toto zobrazenie, nie je samozrejmé, či je konštruovateľné. Z toho plynie, že môže existovať ordinálne číslo, ktoré nie je kardinálne, ale v zmysle interpretácie ℓ kardinálne je.

Teraz pristúpime k samotnému dôkazu axiómu výberu a hypotézy kontinua v ZF, V = L teórií. K dôkazu hypotézy kontinua je potrebný najskôr dôkaz nasledujúcej vety, ktorej podstata je vo vymedzení štruktúry v jazyku teórie množín. Skúmaním štruktúr špecifického tvaru je možné skúmanie tejto štruktúry nahradiť. V týchto špeciálnych štruktúrach je relácia náležania absolútna a ich univerzum je aj tak množinou tranzitívnou. Ak je y každá neprázdna časť množiny c, pričom má táto časť minimálny prvok v relácií r, tak táto relácia r je *fundovaná na množine* c a značíme

$$\varnothing \neq y \subseteq c \to (\exists z \in y)(y \cap r''\{z\} = \varnothing)$$

V dôsledku axiómu fundovanosti je pre ľubovoľnú množinu b relácia $E \cap b^2$ fundovaná na b. Relácia r musí byť fundovaná na množine a, pokiaľ požadujeme, aby boli izomorfné štruktúry $\langle a, r\rangle$ a $\langle b, E \cap b^2\rangle$. Toto je povinná podmienka vzťahujúca sa na nasledujúcu vetu.

Věta 7.3 *V ZF teórií je dokázateľné, že ak je formálnym modelom formalizácie axiómu extenzionality formálna štruktúra $\langle a, r\rangle$ a ak je relácia r fundovaná na množine a, tak existuje taká tranzitívna množina b, že sú štruktúry $\langle a, r\rangle$ a $\langle b, E \cap b^2\rangle$ izomorfné, pričom je jednoznačne určený aj tento izomorfizmus, aj množina b.*

Táto veta sa nazýva **Teorém izomorfizmu** alebo aj **Veta o kolapse**.

Důkaz. V teórií ZF definujeme pre $\alpha \in On$ transfinitnou rekurziou funkcie f_α tak, že:

$$f_0 = \varnothing$$

$$f_{\alpha+1} = f_\alpha \cup \{\langle y, x\rangle; x \in (a - Dom(f_\alpha)) \wedge r''\{x\} \subseteq Dom(f_\alpha) \wedge y = f''_\alpha r''\{x\}\}$$
(pre ľubovoľné ordinálne číslo α)

$$f_\lambda = \bigcup\{f_\alpha; \alpha \in \lambda\}$$
(pre ľubovoľné limitné ordinálne číslo λ)

Pre ľubovoľné $x \in a$ musí existovať α taká, že $x \in Dom(f_\alpha)$

Ak by neexistovala, dalo by sa v relácií r zvoliť $\tilde{x}$ minimálne s takouto vlastnosťou. Znamenalo by to zvoliť $\tilde{x} \in a$ také, že $(\forall z)[z \in r''\{\tilde{x}\} \to (\exists\alpha)(z \in Dom(f_\alpha))] \wedge (\forall\alpha)(\tilde{x} \notin Dom(f_\alpha))$, ale potom je $r''\{\tilde{x}\}$ množinou a to znamená, že podľa schémy nahradenia existuje taká $\alpha \in On$, že by platilo $r''\{\tilde{x}\} \subseteq Dom(f_\alpha)$. Vtedy ale musí byť podľa definície $\tilde{x} \in Dom(f_{\alpha+1})$, čiže dostávame spor.

Keďže a je množina, v dôsledku schémy nahradenia musí existovať $\gamma \in On$ taká, že $(\forall\beta \ni \gamma)(f_\gamma = f_\beta)$, preto je množinou $f = \bigcup\{f_\alpha; \alpha \in On\}$. Z toho vyplýva, že aj obor hodnôt funkcie f je množinou, ktorú označíme b, zapisujeme

$b = Rng(f)$

Ak by nebola funkcia f prostá, existovali by navzájom rôzne $x, y \in a$, pričom by platilo $f(x) = f(y)$. Potom by ale mohlo byť opäť zvolené $\tilde{x}$ minimálne s touto vlastnosťou, čiže by platilo:

$(\forall z)[\langle z, \tilde{x}\rangle \in r \rightarrow (\forall z' \in a)(z \neq z' \rightarrow f(z) \neq f(z'))] \wedge (\exists y \in a)(\tilde{x} \neq y \wedge f(\tilde{x}) = f(y))$ Zafixujeme ešte aj také y. Keďže je splnená formalizácia axiómu extenzionality vo formálnej štruktúre $\langle a, r\rangle$, je $r''\{\tilde{x}\} \neq r''\{y\}$, čiže kvôli zvoleniu množiny $\tilde{x}$ nemôže nastať $f''r''\{\tilde{x}\} = f''r''\{y\}$, pretože ak je napríklad $z \in r''\{\tilde{x}\} - r''\{y\}$, potom $f(z) \in f(\tilde{x})$. Keby $f(z) \in f(y)$, tak by muselo existovať $z' \in r''\{y\}$ také, že by platilo $f(z) = f(z')$. To ale nie je možné kvôli našej voľbe, čiže nastáva spor. Zobrazenie f je izomorfizmus štruktúr $\langle a, r\rangle$ a $\langle b, E \cap b^2\rangle$, keďže podľa definície $f_{\alpha+1}$ je $(\forall x \in Dom(f_{\alpha+1}))(\langle z, x\rangle \in r \equiv f_{\alpha+1}(z) \in f_{\alpha+1}(x))$. Existuje $x \in a$ také, že $y = f_{\alpha+1}(x)$, ak je $y \in Rng(f_{\alpha+1})$, potom ale

$y = f''_{\alpha+1}r''\{x\}$, čiže platí $y \subseteq b$

a tak sme tranzitivitu množiny b dokázali. Ak budeme predpokladať, že medzi štruktúrami $\langle a, r\rangle$ a $\langle b_1, E \cap b_1^2\rangle$ (kde b_1 je tranzitívne) súčastne existuje izomorfizmus $h \neq f$, aby sme získali spor, fixujeme v relácií r $\tilde{x}$ minimálne a také, že platí $f(\tilde{x}) \neq h(\tilde{x})$. Potom ale $f(\tilde{x}) = f''r''\{\tilde{x}\} = h''r''\{\tilde{x}\} \subseteq h(\tilde{x})$. Posledná inklúzia platí v dôsledku predpokladu, že h je izomorfizmus. Ak $e \in h(\tilde{x}) - f(\tilde{x})$, potom existuje $y \in a$ taký, že keďže platí, že je tranzitívne $Rng(h)$, tak $h(y) = e$ a keďže h je izomorfizmus, tak navyše aj $\langle y, \tilde{x}\rangle \in r$. Vtedy ale $h(y) = f(y) \in f(\tilde{x})$. To je ale v rozpore s predpokladom.

■

Věta 7.4 *Axióm výberu a zobecnená hypotéza kontinua sú dokázateľné v ZF, V = L teórií.*

Postupne sa pokúsime vo viacerých krokoch túto vetu dokázať.

Důkaz. Začneme dôkazom axiómu výberu. Ukážeme, že dobré usporiadanie $<<$ možno definovať formulou a to naraz na celej univerzálnej triede, nie len na každej samotnej množine. Zadefinovanie dobrého usporiadania $<<$ spravíme tak, že stanovíme $x << y$, ak $\alpha \in On$ tak, že $x \in L_\alpha \wedge y \notin L_\alpha$. To získame popísaním ostrého usporiadania množiny $L_{\alpha+1} - L_\alpha$ každého $\alpha \in On$ pri predpoklade $(\forall x)(\exists\alpha)(x \in L_{\alpha+1} - L_\alpha)$. Rekurziou podľa ordinálnych čísel získame popis takéhoto usporiadania. K tomu si musíme uvedomiť, že je jednoznačne určený počet formálnych premenných, ktoré majú voľný výskyt vo formálnej formuli a taktiež musíme predpokladať, že L_α už dobre usporiadané je.

Na začiatok usporiadajme množinu usporiadaním $\lhd$: $\{\langle \pi, x_1, ..., x_n \rangle; \pi \in Form \wedge x_1, ..., x_n \in L_\alpha \wedge$ „práve n formálnych premenných má voľný výskyt vo formálnej formuli π“ $\}$. Množinu sme usporiadali lexikograficky vzhľadom k predpokladanému dobrému usporiadaniu na množine L_α a k dobrému usporiadaniu na množine formálnych formulí. Definujeme $x << z$ na základe usporiadania $\lhd$, kde pre $x, z \in L_{\alpha+1} - L_\alpha$. Vzťah $x << z$ platí práve keď existuje formálna formula π, ktorá má práve $n+1$ voľných formálnych premenných $y, x_1, ..., x_n$ a existujú $x_1, ..., x_n \in L_\alpha$ také, že platí nasledujúca formula, ktorá reprezentuje dokázateľnosť axiómu výberu v ZF, L = V teórií.

$$x = \{y \in L_\alpha; \langle L_\alpha, E \cap L_\alpha^2 \rangle \models \pi[y, x_1, ..., x_n]\} \wedge (\forall \varrho)(\forall z_1, ..., z_m \in L_\alpha)(\langle \varrho, z_1, ..., z_m \rangle \lhd \langle \pi, x_1, ..., x_n \rangle \to z \neq \{y \in L_\alpha; \langle L_\alpha, E \cap L_\alpha^2 \rangle \models \varrho[y, z_1, ..., z_m]\})$$

Preskúmanie mohutnosti množín $L_{\in}\alpha$ v ZF teórií je vhodným krokom na dokázanie hypotézy kontinua. Platí, že každé L_α je dobre usporiadané, čiže má mohutnosť, ktorá je kardinálnym číslom. L_α je konečné pre $\alpha \in \omega$, pretože je samozrejmé, že $L_0 = \varnothing$ je konečná a keďže je iba konečne veľa všetkých častí konečnej množiny, tak platí, že konečnosť $L_\alpha \to$ konečnosť $L_{\alpha+1}$. Keďže množina L_ω obsahuje ω a je spočítateľným zjednotením konečných množín, pričom z dôkazu axiómu výberu vyplýva, že je k dispozícií, tak zjednotenie najviac spočítateľne veľa najviac spočítateľných množín je tiež najviac spočítateľná množina, takže z toho usudzujeme, že množina L_ω je spočítateľná. Že má množina L_α rovnakú mohutnosť, ako množina α, pre ľubovoľné $\alpha \ni \omega$, odvodíme indukciou. Mohutnosť menšiu alebo rovnú mohutnosti množiny $Form \times \bigcup\{(L_\alpha)^n; n \in \omega\}$ má množina $L_{\alpha+1}$. Platí, že $(L_\alpha)^n$ má rovnakú mohutnosť ako L_α, pre $0 \in n \in \omega$. Množinu $(L_\alpha)^0$ považujeme za jednoprvkovú.

Množina L_α je pre limitné α zjednotením takého počtu množín, koľko je mohutnosť ordinálneho čísla α. Podľa indukčného predpokladu je mohutnosť každej takejto množiny rovná maximálne mohutnosti ordinálneho čísla α. Vzhľadom k tomu je pre limitné α mohutnosť L_α maximálne rovná mohutnosti ordinálneho čísla α. Pritom ale podľa formule (3) Vety 1 platí $\alpha \subseteq L_\alpha$, takže L_α má prinajmenšom mohutnosť rovnakú, ako α.

Teraz sa sústredíme na dôkaz zobecnenej hypotézy kontinua v ZF, V = L teórií. Predstavme si ľubovoľnú nekonečnú mohutnosť $\aleph_\alpha$, pričom $\alpha \in On$. Potrebujeme preukázať, že mohutnosť $P(\aleph_\alpha)$ je najviac $\aleph_{\alpha+1}$. Podľa odhadu mohutností množín L_β k tomu stačí dokázať $e \subseteq \aleph_\alpha \to e \in L_{\aleph\alpha+1}$, kde e bude akákoľvek časť $\aleph_\alpha$. Z predpokladu koštruovateľnosti každej množiny usudzujeme, že musí existovať taká β, že platí $e \in L_\beta$, pričom zatiaľ nevieme, ako veľké je najmenšie ordinálne číslo β, ktoré má túto vlastnosť. Chceme preukázať, že to najmenšie je práve prvkom $\aleph_{\alpha+1}$.

Zvolíme formulu φ s dvomi premennými x, y, pre ktorú platí $\varphi(x, y) \to (x \in L_y \wedge (\forall x, y)[x = y \equiv (\forall e)(e \in x \equiv e \in y)])$ (pripomenieme, že formula v konjunkcii napravo je axióm extenzionality), ďalej vložíme všetky vlastnosti nutné ku konštrukcii uvedeného vzťahu do φ. Napríklad je takou vlastnosťou $Ord(y)$. Na začiatok vytvoríme štruktúru $\langle a, r \rangle$ s vlastnosťami

- (1) $r = E \cap a^2$, teda $\langle a, r\rangle$ je podštruktúrou štruktúry $\langle V, E\rangle$
- (2) $\aleph_\alpha \subseteq a$ a súčastne $e, \beta \in a$
- (3) a má najviac $\aleph_\alpha$ mohutnosť
- (4) $\langle a, r\rangle \models \varphi[x \longmapsto e, y \longmapsto \beta]$

Na zaručení vlastnosti definovanej v bode (4) je založená obtiažnosť celej konštrukcie. Dosiahneme toho tak, že postupne vytvoríme množiny a_m pre ktoré platí, že $m \in \omega$. Prihliadame pritom, aby všetky mali mohutnosť najviac $\aleph_\alpha$. Množinou a, teda bude $\bigcup\{a_m; m \in \omega\}$. Je splnená požiadavka vlastnosti (3) a vlastnosť (2) dosiahneme tak, že definujeme $a_0 = \aleph_\alpha \cup \{e\} \cup \{\beta\}$, pričom je jasné, že množina a_0 má mohutnosť najviac $\aleph_\alpha$. Pre $m \in \omega$ budeme predpokladať, že je už zkonštruované a_m a ideme zostrojiť a_{m+1}. Overme, či pre ľubovoľné $x_1, ..., x_n \in a_m$ a ľubovoľnú podformulu ψ formule φ s voľnými premennými $y, z_1, ..., z_n$ jazyka teórie množín existuje taká množina $\tilde{y}$, že $\psi(y/\tilde{y}, z_1/x_1, ..., z_n/x_n)$. Ak takáto $\tilde{y}$ množina existuje, pridáme do množiny a_{m+1} jednu množinu s danou vlastnosťou tak, že je usporiadaním popísaným v prvej časti dôkazu definované jediné $\tilde{y}$ pre ľubovoľnú myslenú formulu ψ a ľubovoľné parametre, teda to najmenšie a tak toto $\tilde{y}$ pridáme. Zároveň netvrdíme, že inou vlastnosťou ψ' nepridáme ešte iné $\tilde{y}'$ také, že má tiež vlastnosť ψ. Najmenšou nadmnožinou množiny a_m, ktorá obsahuje takto pridané prvky pre všetky mysliteľné podformule formule φ a všetky možné parametre z a_m bude teda množina a_{m+1}. Taktiež mohutnosť a_{m+1} je najviac $\aleph_\alpha$, keďže všetkých možných parametrov je najviac $\aleph_\alpha$. Podmienku (1) zaručíme definovaním $r = E \cap a^2$.

Poslednú podmienku (4) splníme pomocou indukcie podľa zložitosti podformúl ψ formule φ, do ktorých sú dosadené parametre z a. Vzhľadom k definícií relácie r nie je čo preukazovať, ak je ψ základnou formulou. Základným dôsledkom definície splňovania v štruktúre sú indukčné kroky implikácie a negácie. Konštrukcia formule $(\exists z)\psi \rightarrow (\exists z \in a)\langle a, r\rangle \models \psi[y \longmapsto z]$ zabezpečuje jednu potrebnú implikáciu indukčného kroku kvantifikácie. Implikácia vo formuli $(\exists z \in a)\langle a, r\rangle \models \psi[y \longmapsto z] \rightarrow (\exists z)\psi$ je triviálna.

Vlastnosť (4) zaručuje, že je splnená formalizácia axiómu extenzionality v štruktúre $\langle a, r\rangle$. Z dôkazu Vety 3 vyplýva, že existuje tranzitívna množina b a izomorfizmus f štruktúr $\langle a, r\rangle$ a $\langle b, E \cap b^2\rangle$, ktorý je určený na celej množine a, ktorej súčasťou je kardinálne číslo $\aleph_\alpha$. Predvedieme, že $(\forall \xi \in \aleph_\alpha)(\xi = f(\xi))$, pričom ak by to neplatilo, mohli by sme ako najmenšie ordinálne číslo $\xi \in \aleph_\alpha$, pre ktoré platí $\xi \neq f(\xi)$, zafixovať ζ. Vtedy ale $\delta \in \zeta \rightarrow \langle \delta, \zeta\rangle \in r$. Preto $\langle f(\delta), f(\zeta)\rangle \in E \cap b^2$, teda $\delta = f(\delta) \in f(\zeta)$, takže $\zeta \subseteq f(\zeta)$. Ak $x \in f(\zeta)$, potom $x \in b$ kvôli tranzitivite množiny b. Musí existovať $y \in a$ tak, že platí $f(y) = x$. Avšak vtedy $\langle y, \zeta\rangle \in r$, takže $y \in \zeta$. Potom $x = f(y) = y \in \zeta$, ciže sme preukázali $\zeta = f(\zeta)$, čo vedie ku sporu. Pravdivosť formálnej formule sa vo formálnej štruktúre prenáša izomorfizmom, takže platí $\langle b, E \cap b^2\rangle \models \varphi[x \longmapsto f(e), y \longmapsto f(\beta)]$. Vieme aj, že $f(e) = e$. Z výskumu v dôkaze Vety 2 plynie, že všetky potrebné formule sú absolútne, keďže je b tranzitívne. Ilustračne máme ekvivalenciu $Ord(f(\beta)) \equiv \langle b, E \cap b\rangle \models Ord(z)[z \longmapsto f(\beta)]$, ale pritom je mohutnosť $f(\beta)$ menšia alebo rovná mohutnosti množiny b, pričom platí, že b má mohutnosť najviac $\aleph_\alpha$, preto $f(\beta) \in \aleph_{\alpha+1}$.

Stačí si už iba uvedomiť platnosť $(\langle b, E \cap b^2\rangle \models \varphi[x \longmapsto f(e), y \longmapsto f(\beta)]) \rightarrow e = f(e) \in L_{f(\beta)}$. Tým je dokončený dôkaz, že ani AC, ani GCH nie je možné v ZF vyvrátiť, teda pomocou konštrukcie Gödelových konštruovateľných množín sa dá dokázať relatívna bezospornosť axiómu výberu a zobecnenej hypotézy kontinua s teóriou ZF. ∎

Je možné zobecniť konštrukciu konštruovateľných množín spôsobom, že zadefinovaním triedy $L[x]$ pre $x \subseteq L$ tak, že $x \in L[x]$, pričom sú vlastnosti triedy $L[x]$ obdobné vlastnostiam triedy L. Je možné demonštrovať, že napríklad ak existuje $x \subseteq \omega \wedge x \notin L$, tak vzťah V = L neplatí, pričom zobecnená hypotéza kontinua v zmysle interpretácie definovanej pomocou triedy $L[x]$ platí.

K spracovaniu tejto kapitoly nám poslúžili zdroje [4], [2].

8 Záver

V úvode práce sme sa zaoberali definíciou logickej teórie, zadefinovali sme jednotlivé pojmy, s ktorými sme neskôr potrebovali pracovať a popísali vzťahy medzi nimi.

Ďalšia časť práce popisuje okolnosti, kvôli ktorým bolo nevyhnutné vytvoriť nad naivnou teóriou množín komplikovanejší a prepracovanejší systém a postaviť tak teóriu množín na pevné axiomatické základy, v ktorých už paradoxy naivnej teórie množín nemajú platnosť.

Detailnejšiemu preskúmaniu a popísaniu vzťahov v takýchto axiomatických systémoch sa venuje ďalšia kapitola. Sú tu spracované tri najznámejšie a najpoužívanejšie axiomatické teórie množín, s popisom ich axiomatického systému. Z tejto kapitoly je evidentné, že Zermelo-Fraenkelova teória množín je základnou axiomatickou teóriou množín a v literatúre zaoberajúcou sa problematikou teórií množín je najčastejšie sa vyskytujúcou. Čo sa týka Kelley-Morseovej teórie množín, je možné konštatovať, že táto teória je špeciálnym prípadom Gödel-Bernaysovej teórie množín, keďže jej axiomatický systém je až na jeden axióm totožný.

Táto malá zmena, je ale zmenou rozsiahlejšou. Je to možné pozorovať v ďalšej kapitole, kde sme ukázali formulu, ktorá je dokázateľná v Kelley-Morseovej teórií množín, ale nie je dokázateľná v Zermelo-Fraenkelovej teórií množín. Z toho môžeme vyvodiť záver, že Kelley-Morseová teória množín je silnejšia ako Zermelo-Fraenkelová teória množín.

Ďalšia kapitola bola zameraná na preukázanie, že Gödel-Bernaysovú teóriu množín je možné upraviť na teóriu s konečne veľa axiómami a tak z nej vytvoriť Finítnu verziu Gödel-Bernaysovej teórie množín. Toto je prekvapivý výsledok, pretože schéma existencie tried v štandardnej Gödel-Bernaysovej teórií množín zaručuje pridanie axiómu existenciu triedy množín s určitou vlastnosťou pre každú novú formulu a teda sa javí, že táto schéma zaručuje nekonečne veľa axiómov. V tejto kapitole je však podaný návod, ako je možné túto schému eliminovať.

Posledná kapitola sa venuje naozaj dôležitým dôkazom v teórií množín - preukázaniu relatívnej bezospornosti axiómu výberu a hypotézy kontinua so Zermelo-Fraenkelovou teóriou množín pomocou konštrukcie konštruovateľných množín popísaných Kurtom Gödelom. Takže za predpokladu, že sú axiómy Zermelo-Fraenkelovej teórie množín bezosporné, pridaním hypotézy kontinua a axiómu výberu vznikne opäť bezosporný systém axiómov. Pre doplnenie uvedieme, že Paul Cohen v roku 1963 preukázal, že ak sú axiómy teórie množín bezosporné, potom z nich ani s použitím axiómu výberu nie je možné hypotézu kontinua dokázať. [4] Z Gödelových a Cohenových výsledkov je teda jasné, že na základe axiómov teórie množín nie je možné hypotézu kontinua rozhodnúť. Čo sa týka axiómu výberu, mnoho matematikov ho odmieta, pretože na rozdiel od ostatných axiómov, ktoré majú konštrukčný charakter, axióm výberu nedáva žiadnu predstavu, ako vyzerá jeho výberová funkcia. Dalo by sa teda zhodnotiť, že má len charakter existenčný. Napriek tomu sa jeho praktická aplikácia dá nájsť v dôkazoch tvrdení, na ktorých sú postavené mnohé matematické odvetvia.

Práca teda podáva prehľadný a ucelený pohľad na najpoužívanejšie axiomatické teórie množín s popisom dôkazov vybraných teorémov vrámci konkrétnych teórií, pričom je v úvode objasnený dôvod vzniku axiomatických teórií množín a popísaná výstavba logickej teórie. Tým sa tento materiál stáva užitočným pre poslucháčov predmetu Vybrané partie z logiky za účelom rozširovania vedomostí z oblasti teórie množín.

9 Reference

[1] Balcar, Bohuslav; Štěpánek, Petr, *Teorie množin*, 2. vydanie, Academia, Praha, 2001.

[2] Sochor, Antonín, *Metamatematika teorií množin*, Univerzita Karlova v Praze, Praha, 2005.

[3] Duží, Marie, *Logika pro informatiky* - skriptá VŠB-TU Ostrava, 2012, Dostupné na: `http://www.cs.vsb.cz/duzi/Matlogika_ESF_Definite.pdf`, Dátum: [30.3.2014].

[4] Cohen, Paul, *Set theory and the continuum hypothesis*, Dover Publications, New York, 2005.

[5] Vopěnka, Petr, *Úvod do klasické teorie množin*, Vydavatelství Západočeské univerzity v Plzni, Plzeň, 2011.

[6] Šalát, Tibor; Smítal, Jaroslav, *Teória množín*, Alfa, Bratislava, 1986.

[7] Mareš, Jan, *Teorie množin* - skriptá ČVUT Praha, 2008, Dostupné na: `http://people.fjfi.cvut.cz/maresjan/ke_stazeni.html`, Dátum: [12.4.2014].

[8] Wikipedia, *Cantorova věta*, Dostupné na: `http://cs.wikipedia.org/wiki/Cantorova_věta`, Dátum: [1.5.2014].

[9] Bartl, David, *Úvod do teorie množin a logiky 2* - skriptá OU Ostrava, 2008, Dostupné na: `http://www1.osu.cz/~bartl/publs/?index=0085&fullt=20`, Dátum: [24.4.2014].

[10] Wikipedia, *Von Neumannova-Bernaysova-Gödelova teorie množin*, Dostupné na: `http://cs.wikipedia.org/wiki/Von_Neumannova-Bernaysova-Gödelova_teorie_množin`, Dátum: [5.4.2014].